Reference: ASSR-2023-CB-Exploit Pack

Master Cryptis 2023
ASSR

Université de Limoges
NAME : Salame Joe

Exploit Pack Cookbook

Summary

In today’s dynamic and interconnected digital environment, the use of penetration testing tools has become crucial for organizations aiming to fortify their cybersecurity defenses. These tools play an important role in proactively identifying and mitigating vulnerabilities to ensure a resilient and secure infrastructure against constantly evolving cyber threats.

This is where our Cookbook comes in handy as we provide you an in-depth guide to the powerful penetration testing tool, Exploit Pack. We will present Exploit Pack while highlighting its various advantages and features. Furthermore, we will discover how integrating this offensive tool in cybersecurity practices enhances the proactive identification and mitigation of potential threats. The Cookbook concludes with a user-friendly, step by step implementation guide of the trial version of Exploit Pack, guaranteeing a seamless deployment on a Linux environment. Finally, a straightforward yet impactful test will be conducted to show the deployment and execution of an exploit.

General Presentation:

As technological advancement continues to evolve, businesses increase their dependency on information technology thereby amplifying the emergence of new threats and vulnerabilities that can be exploited by cybercriminals. This is where the use of penetration testing and exploit tools are essential to address cyber threats and ensure robust cybersecurity defenses through simulated attacks.

Ethical penetration and offensive exploit tools are considered crucial components of cybersecurity. They involve authorized attempts to breach system security to identify vulnerabilities that a malicious hacker can exploit. They consist of tools, exploits, vulnerability scanners, network sniffers, and more. They allow organizations to simulate an attack on their IT infrastructure to identify various vulnerabilities before a malicious actor does.

Among these tools and frameworks, Exploit Pack emerges as the next generation offensive tool designed since 2008 to address any security professionals seeking to test their digital infrastructure. It allows you to develop your own exploits or to make use of their 39500+ exploits, if you purchase a license, in order to test the security of targets depending on their type. For the free version, you will get around 450 exploits.

Exploit Pack is equipped with a range of features to help cybersecurity professional and penetration testers to enhance overall security posture of systems and network. Some of these features are the wide range of Exploits that we mentioned earlier, Post-exploitation Modules, Automation and Scripting, Network Scanning with Nmap, Target Specific Modules, Reporting and Logging, community and Support and many more. This framework goes beyond simulation, offering tools to attack, take control, bypass security measures and ensure persistence while operating discreetly. To be able to access all these functionalities and features, Exploit Pack offers two license options, one-year and two-year license. The framework is Java based GUI tool that can be installed on Linux, Windows and Mac OS and it requires the Java package to run on the host in order to work.

Definitions:

Exploit Pack, advanced exploitation framework that provides the capabilities to develop custom exploits or leverage a vast collection of public exploits available in its lab. Its purpose is to help penetration testers, red teams and cyber security professionals to detect threats and test their organization's digital infrastructure.

Here is some key terms and terminology you need to know:

1. **Exploits**
   - Codes designed to take advantage of vulnerabilities in systems, networks or applications.
2. **Modules**:
   - Pre-built components and scripts used to perform specific tasks such as launching exploits or conducting scans.
3. **Network Mapper (Nmap)**:
   - Open-source tool for network discovery and security auditing.
4. **Targets**:
   - Systems or applications where the penetration testing will be executed. Mainly they are specific software versions or configurations.
5. **Shellcode**:
   - Code used to inject and execute commands on a target.
6. **Shell Execute**:
   - Feature to facilitate the execution of shell commands on a targeted system.

Hardware and Software Prerequisites:

In order to successfully implement and test Exploit Pack, please ensure you have the following Hardware and Software ingredients:

Hardware Prerequisites:

1. **Server/Computer:** We will use a VirtualBox VM.
2. **Storage Spaces:** At least 30GB of disk space are required for your VM in which 500MB are for Exploit Pack.
3. **CPU:** At least 2 CPU are required for our testing environment.
4. **RAM:** At least 4 GB of memory.

Software Prerequisites:

1. **Linux OS:** We will use Ubuntu 22.04.3 LTS as our OS.
2. **Java Software:** A version higher than 8.
3. **Exploit Pack Software :** Exploit Pack v17.
4. **Python:** Version 2.7 and above.

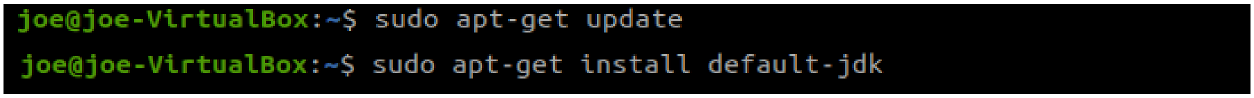
Please note that the target machine in this cookbook is the same machine where we are going to install the exploit Pack trial version. This due to the limitation of this free version, we cannot add another distant target. However, with a full licensed version, you will be able to add other targets.

Illustrative Recipe

Step 1- Installing Exploit Pack

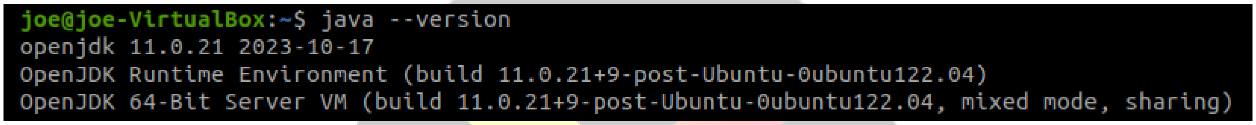
This Section provides step-by-step instructions for installing Exploit Pack on an Ubuntu machine.

To get started, you need to install Java on your machine. As we mentioned in the software requirements the minimum version supported is 8.
Run the following commands to update the list of available packages and to download **Java**:



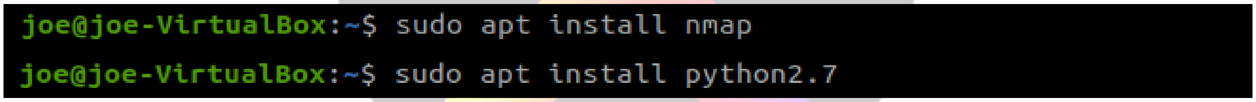
```
joe@joe-VirtualBox:~$ sudo apt-get update
joe@joe-VirtualBox:~$ sudo apt-get install default-jdk
```

Verify if **Java** is properly installed with the following command:



```
joe@joe-VirtualBox:~$ java --version
openjdk 11.0.21 2023-10-17
OpenJDK Runtime Environment (build 11.0.21+9-post-Ubuntu-0ubuntu122.04)
OpenJDK 64-Bit Server VM (build 11.0.21+9-post-Ubuntu-0ubuntu122.04, mixed mode, sharing)
```

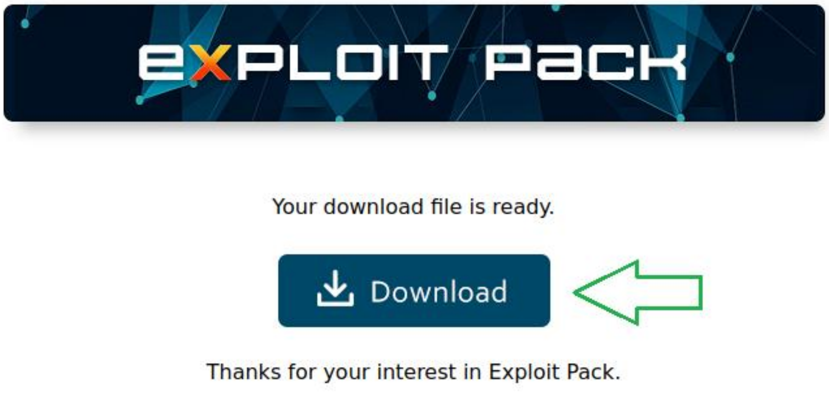
In case you don’t have **Nmap** and **Python** installed on the machine the following commands must be executed:



```
joe@joe-VirtualBox:~$ sudo apt install nmap
joe@joe-VirtualBox:~$ sudo apt install python2.7
```

Open your preferred web browser and download the Exploit Pack package from the official website: https://exploitpack.com/download/release/.

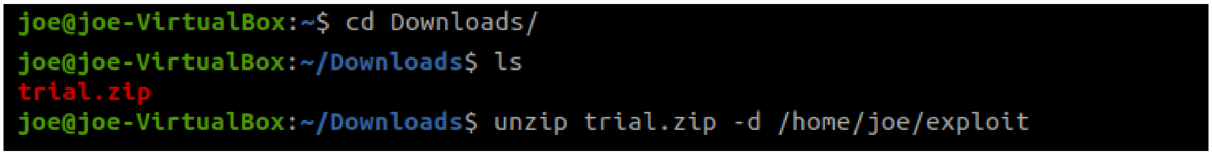
Press the following button to download the zip file **trial.zip:**



Your download file is ready.

Thanks for your interest in Exploit Pack.

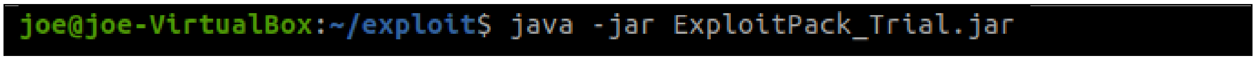
Once completed, run the following command to unzip it:



```
joe@joe-VirtualBox:~$ cd Downloads/
joe@joe-VirtualBox:~/Downloads$ ls
trial.zip
joe@joe-VirtualBox:~/Downloads$ unzip trial.zip -d /home/joe/exploit
```

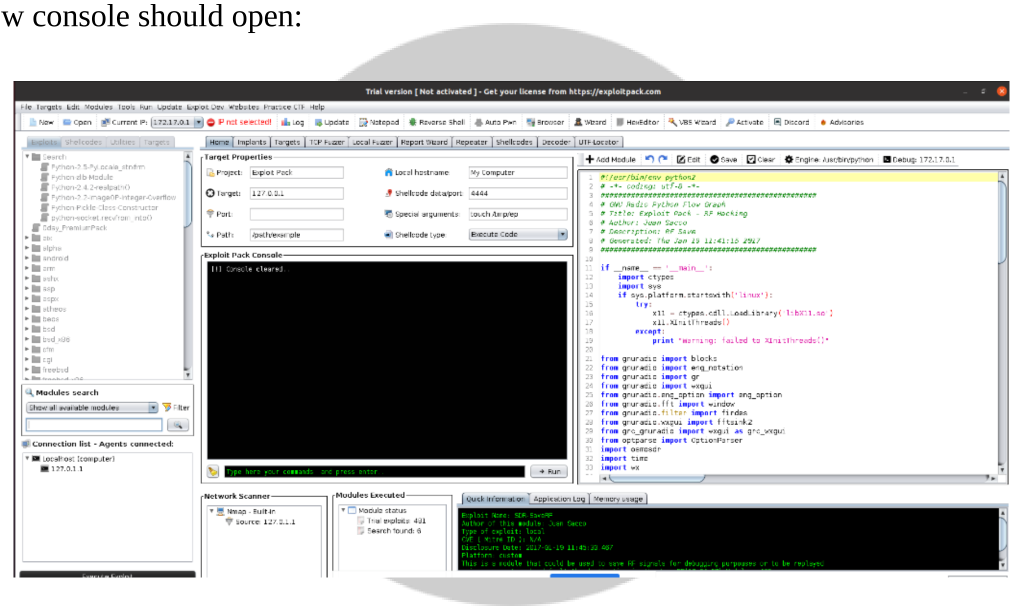
N.B: In the **unzip** command, we chose the path **/home/joe/exploit** but you can choose another location.

Now navigate to the path and start the Exploit Pack by running this command:



```
joe@joe-VirtualBox:~/exploit$ java -jar ExploitPack_Trial.jar
```

The below console should open:



Trial version [Not activated] - Get your license from https://exploitpack.com
File Targets Edit Modules Tools Run Update Exploit Dev Websites Practice CTF Help
New Open Current IP: 172.17.0.1 IP not selected! Log Update Notepad Reverse Shell Auto Pwn Browser Wizard HexEditor VBS Wizard Activate Discord Advisories
Exploits Shellcodes Utilities Targets
Home Implants Targets TCP Fuzzer Local Fuzzer Report Wizard Repeater Shellcodes Decoder UTF-Locator
Add Module Edit Save Clear Engine: /usr/bin/python Debug: 172.17.0.1
Modules search
Show all available modules
Filter
Connection list - Agents connected:
Localhost (computer)
127.0.1.1
Network Scanner
Nmap - Built-in
Modules Executed
Module status
Quick Information Application Log Memory usage

Target Properties
Project: Exploit Pack
Target: 127.0.0.1
Port:
Path: /path/example
Local hostname: My Computer
Shellcode data/port: 4444
Special arguments: touch /tmp/eq
Shellcode type: Execute Code

Exploit Pack Console

```
[!] Console cleared.
Type here your commands  and press enter
```

```
#!/usr/bin/env python2
# -*- coding: utf-8 -*-
##################################################
# GNU Radio Python Flow Graph
# Title: Exploit Pack - RF Hacking
# Author: Juan Sacco
# Description: RF Save
# Generated: Thu Jan 19 11:41:15 2017
##################################################

if __name__ == '__main__':
    import ctypes
    import sys
    if sys.platform.startswith('linux'):
        try:
            x11 = ctypes.cdll.LoadLibrary('libX11.so')
            x11.XInitThreads()
        except:
            print "Warning: failed to XInitThreads()"

from gnuradio import blocks
from gnuradio import eng_notation
from gnuradio import gr
from gnuradio import wxgui
from gnuradio.eng_option import eng_option
from gnuradio.fft import window
from gnuradio.filter import firdes
from gnuradio.wxgui import fftsink2
from grc_gnuradio import wxgui as grc_wxgui
from optparse import OptionParser
import osmosdr
import time
import wx
```

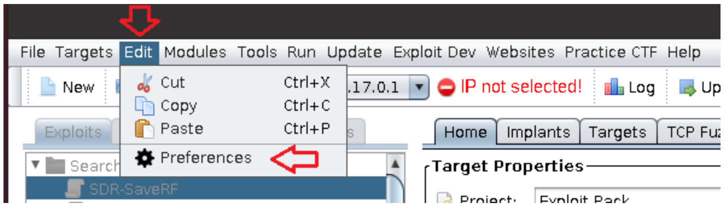
```
Source: 127.0.1.1
Trial exploits: 491
Search found: 6
```

```
Exploit Name: SDR-SaveRF
Author of this module: Juan Sacco
Type of exploit: local
CVE ( Mitre ID ): N/A
Disclosure Date: 2017-01-19 11:45:33.487
Platform: custom
This is a module that could be used to save RF signals for debugging purpouses or to be replayed
```

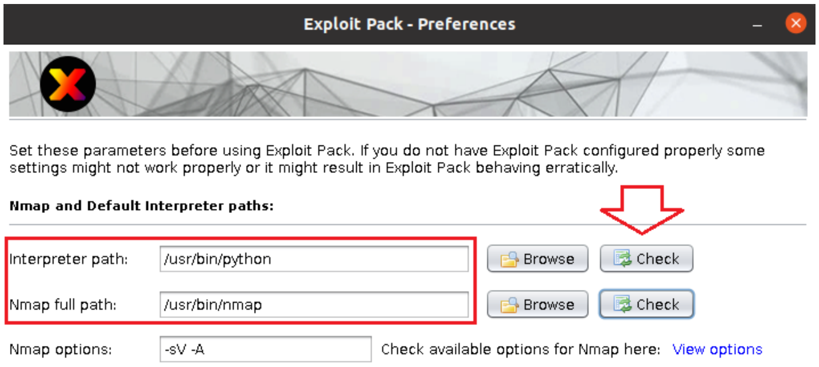
Step 2- Exploit Pack Deployment

Before starting to use Exploit Pack, you must configure your preferences. The main ones required are **Interpreter path** and **Nmap full path**.

To do so, select the **Edit** option from the top bar menu then **Preferences** from the displayed list:



Now in the **Preferences** window make sure the **Interpreter path** and **Nmap full path** are correct by clicking the check button as below. To finish click the **save** button on the bottom of the window:



Set these parameters before using Exploit Pack. If you do not have Exploit Pack configured properly some settings might not work properly or it might result in Exploit Pack behaving erratically.

Nmap and Default Interpreter paths:

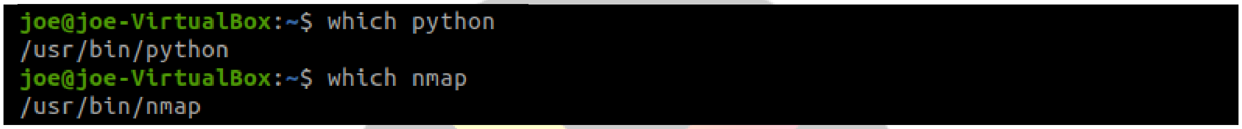
Interpreter path: /usr/bin/python

Nmap full path: /usr/bin/nmap

Nmap options: -sV -A

Check available options for Nmap here:

N.B: If you don’t have the correct paths, run the below commands to get the full path of each:

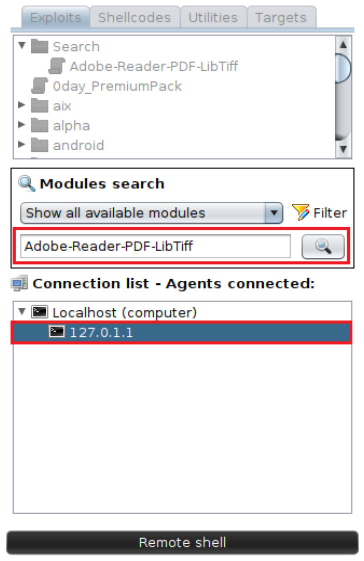


```
joe@joe-VirtualBox:~$ which python
/usr/bin/python
joe@joe-VirtualBox:~$ which nmap
/usr/bin/nmap
```

Step 3- Minimal testing

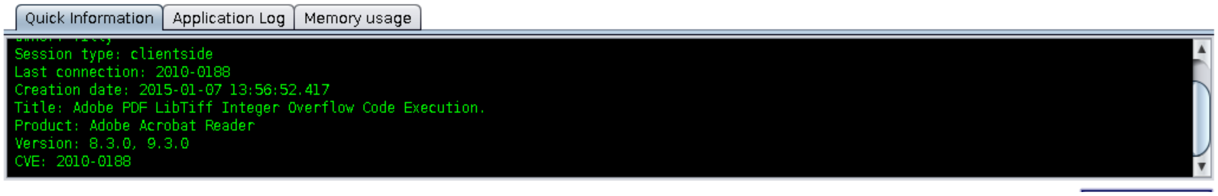
Now, we will proceed to perform a small test using the **Adobe Reader PDF LibTiff** module. The script creates a malicious PDF file that, when opened, exploits the vulnerability to execute arbitrary code.

To begin the test, search for the module on the left bottom. Select the IP localhost and press **Remote shell** button to run the code:



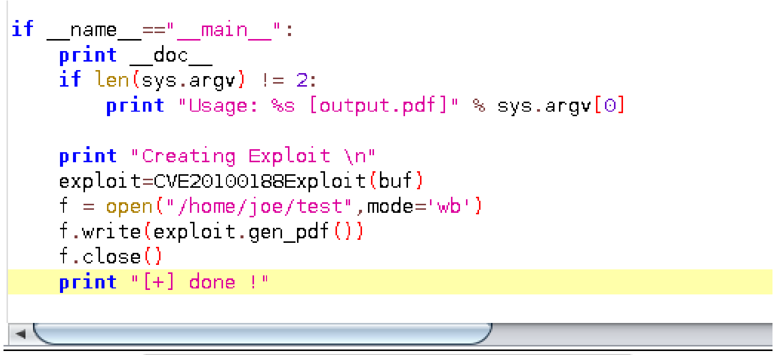
Adobe-Reader-PDF-LibTiff

To check if the module was loaded, the following information should be displayed in the command shell on the right bottom of the screen:



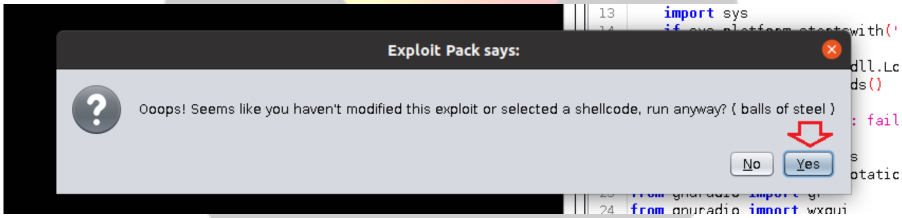
```
Session type: clientside
Last connection: 2010-0188
Creation date: 2015-01-07 13:56:52.417
Title: Adobe PDF LibTiff Integer Overflow Code Execution.
Product: Adobe Acrobat Reader
Version: 8.3.0, 9.3.0
CVE: 2010-0188
```

As you see below, the exploit allows the attacker to create the malicious pdf file. Before running the module, we indicated the path of the file where to be created on the target:



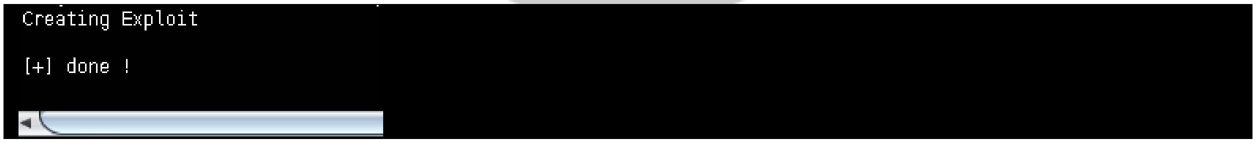
```
if __name__=="__main__":
    print __doc__
    if len(sys.argv) != 2:
        print "Usage: %s [output.pdf]" % sys.argv[0]

    print "Creating Exploit \n"
    exploit=CVE20100188Exploit(buf)
    f = open("/home/joe/test",mode='wb')
    f.write(exploit.gen_pdf())
    f.close()
    print "[+] done !"
```

Finally, to run the module press the **Remote Shell** button then press **Yes** on the displayed window:



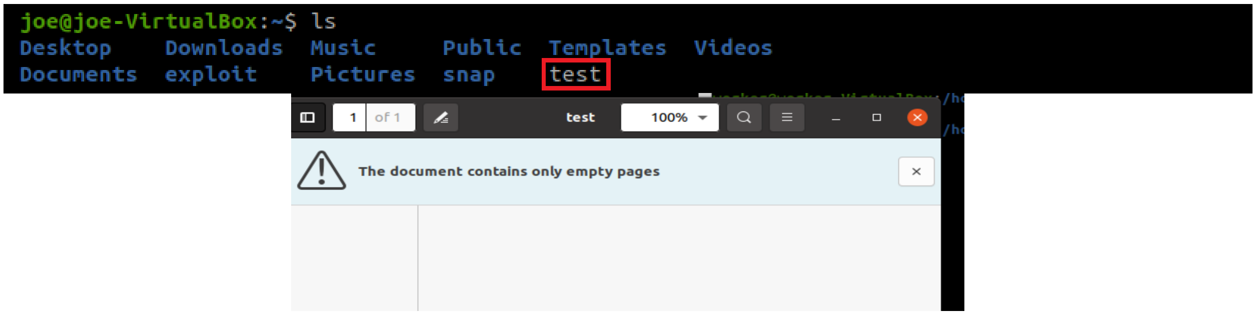
Ooops! Seems like you haven't modified this exploit or selected a shellcode, run anyway? (balls of steel)

You will notice on the **Exploit Pack Console** the following:



```
Creating Exploit

[+] done !
```

Go the target machine, in our case it is the same VM, and check if the file was created and then open it:



```
joe@joe-VirtualBox:~$ ls
Desktop    Downloads  Music     Public  Templates  Videos
Documents  exploit    Pictures  snap    test
```

The document contains only empty pages

References/Documentations:

1. A Guide To Penetration Testing
   https://medium.com/@daytonsteinbach/a-guide-to-penetration-testing-fce9417d6c74
2. Exploit Pack Official website:
   https://exploitpack.com/
3. Juan Sacco git books -Exploit Pack
   https://juansacco.gitbooks.io/exploitpack/content/chapter1.html