

Secure Coding Lab

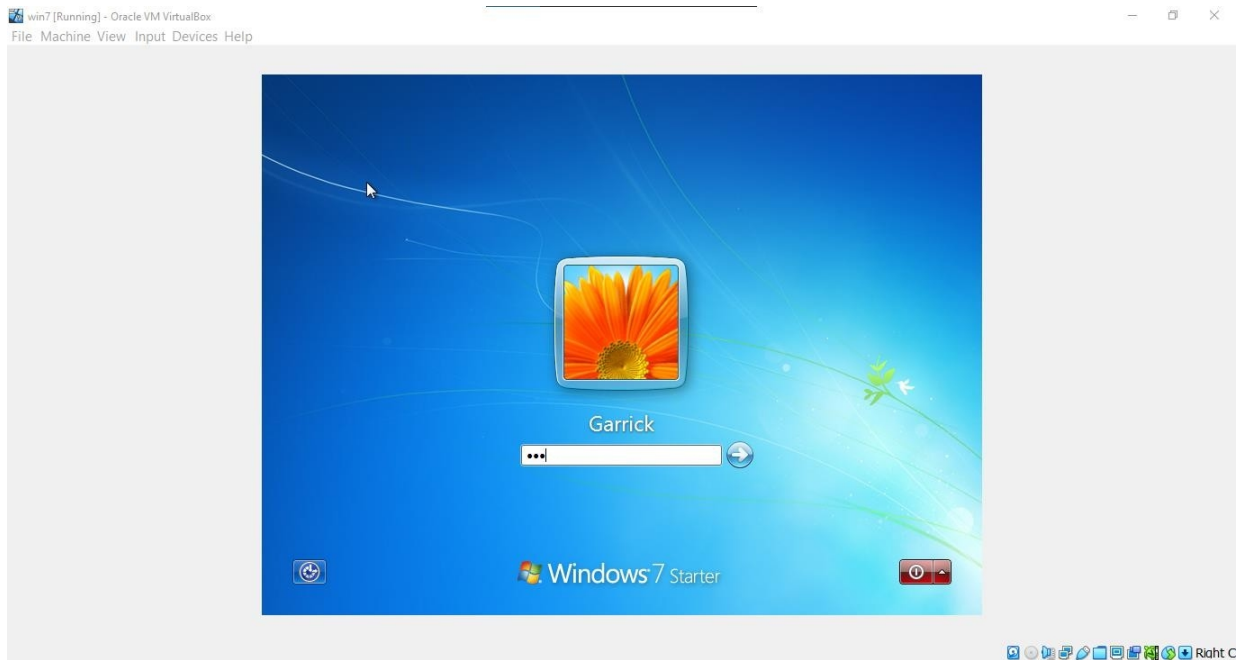
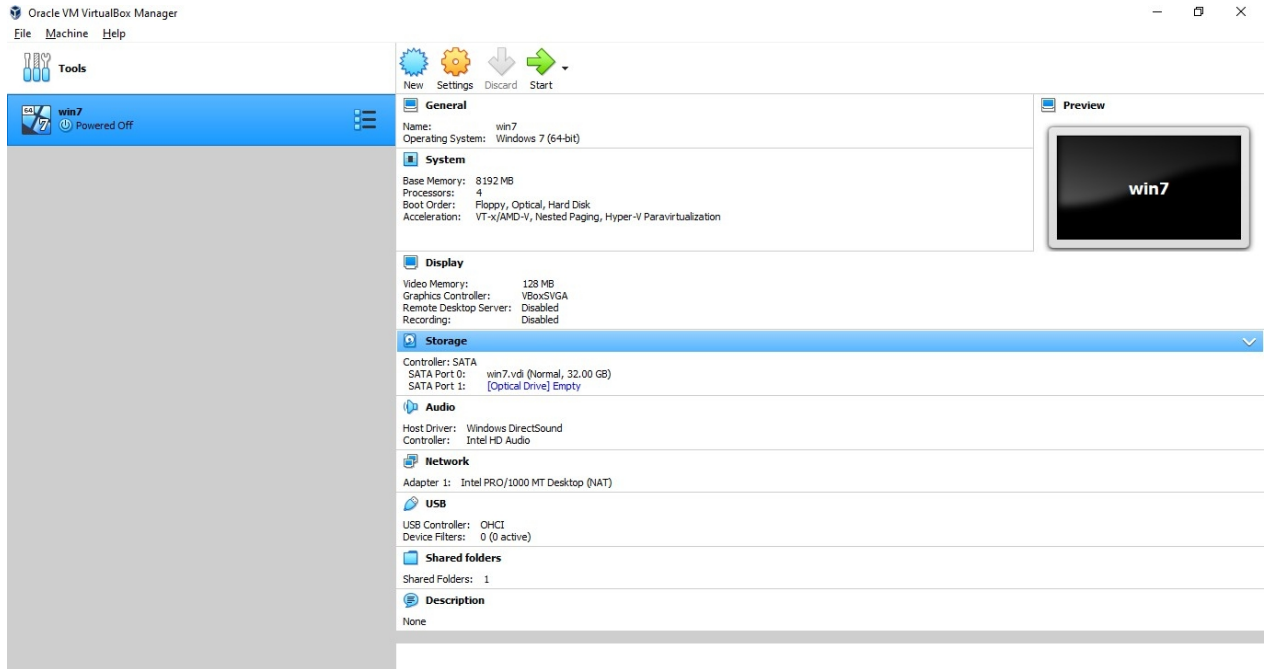
– 7

Khushal Khare

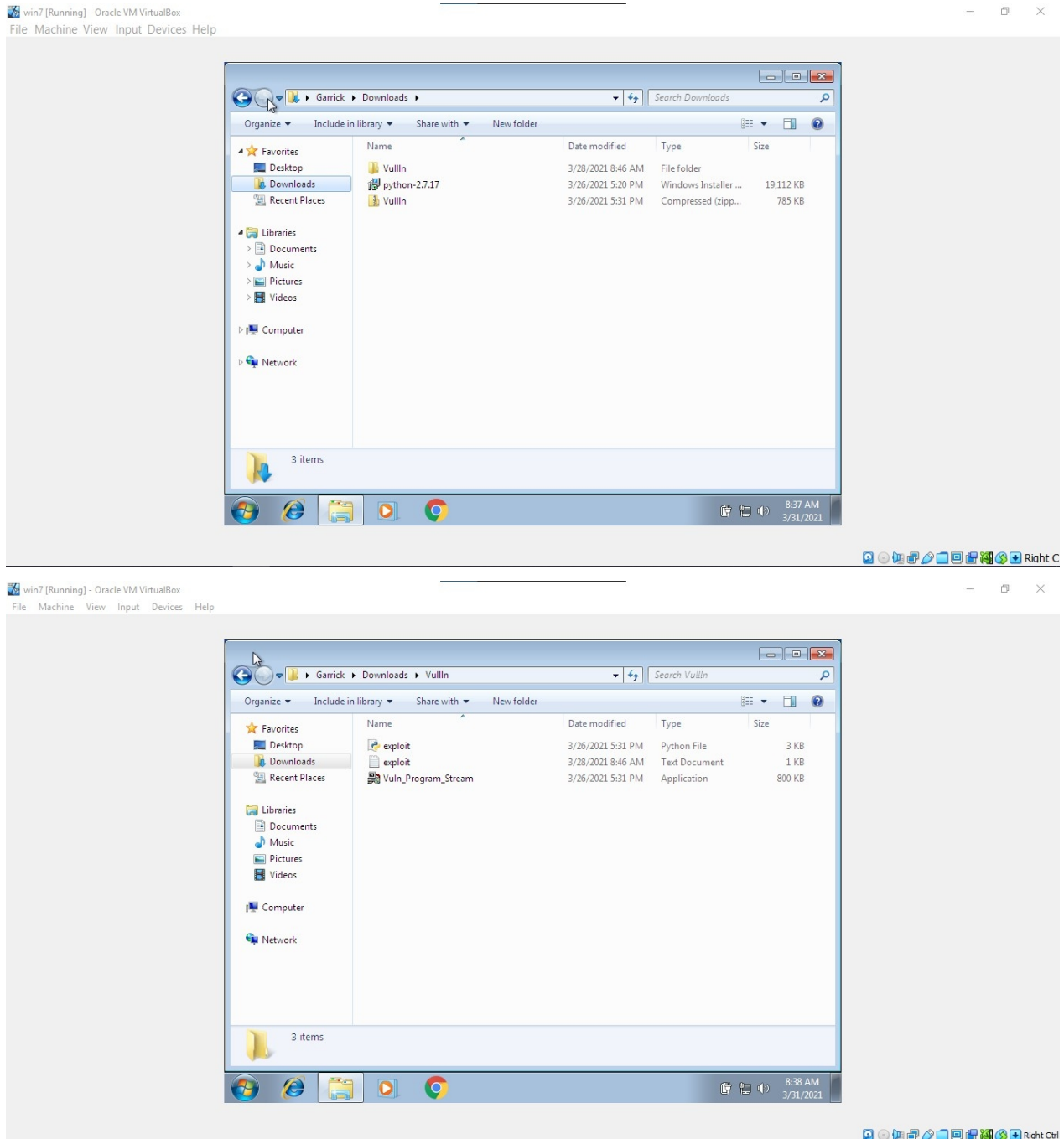
18BCE7036

Install windows 7 on a VM:

VM Configuration

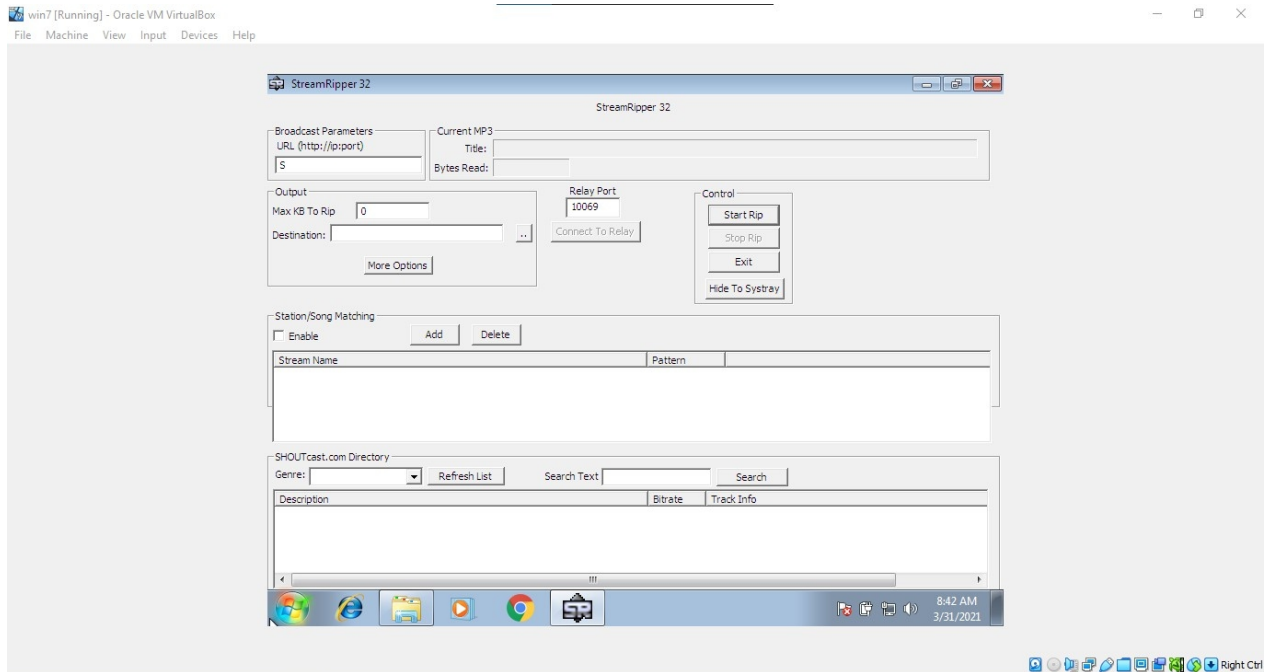


Extract the Zip file to get the application executable and a python file:

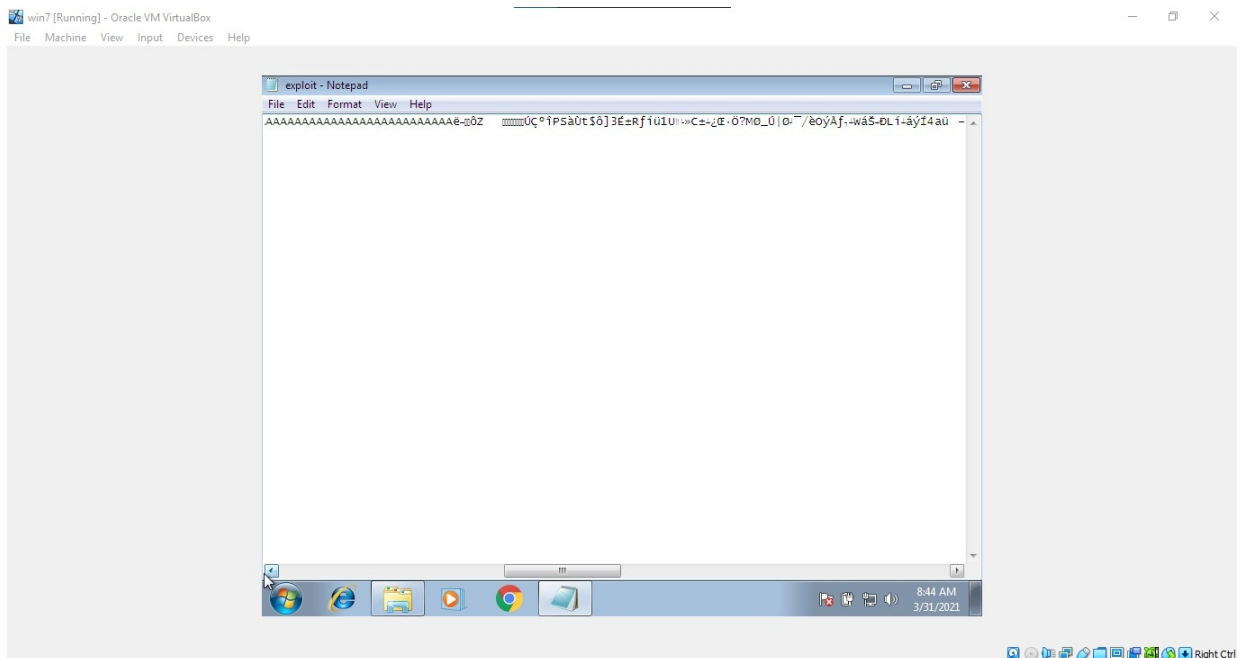


Because this is a fresh install of windows 7 and because official support for windows 7 ended a while ago, we had to install python 2.7.17 and Chrome to download the files and to execute the py file.

The Application we are trying to find a vulnerability is called StreamRipper32:



After executing the python file, we get a new exploit.exe file which has the required payload for the exploit:



The screenshot displays the StreamRipper 32 application window. The interface includes several sections:

- Broadcast Parameters:** Fields for URL (http://ip:port), Title, and Bytes Read.
- Output:** Fields for Max KB To Rip (set to 0) and Destination, along with a More Options button.
- Relay Port:** Set to 10069.
- Control:** A Start Rip button.
- Station/Song Matching:** A checkbox for Enable and an Add button.
- SHOUTcast.com Directory:** A section with a Genre dropdown, Refresh List button, Search Text field, and Search button. Below this is a table with columns for Description, Bitrate, and Track Info.

A **Pattern Match** dialog box is open in the center, showing:

- Station Pattern:** StreamRipper 32
- Song Pattern:** `c^sM c^o4(6s=^0^Y|0CE|l=^*Y|0LGc11:##E|A`
- Note:** All pattern matches are "substring" matches. Use keyword "any_match" to match any station or song.

The Windows taskbar at the bottom shows icons for various applications and the system clock indicating 8:50 AM on 3/31/2021.

Why the Application crashes:

So when the input in that text field exceeds 256 characters, Buffer Overflow happens and that causes the application to crash, because it is not being handled properly.

This vulnerability can be easily fixed by limiting the number of characters that specific field takes or just taking the first 256 characters from that field.