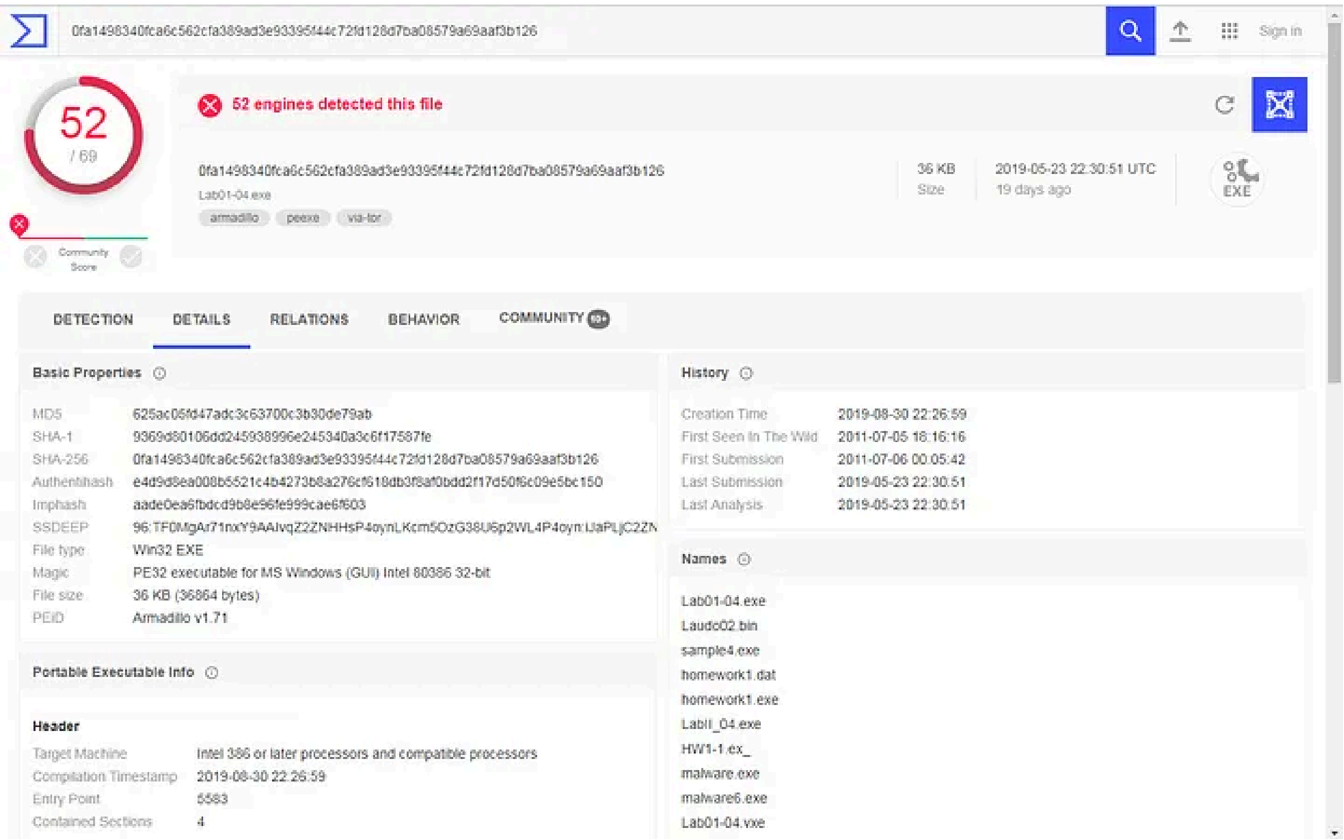
Practical Malware Analysis — Chapter 1 — Lab 01–04 — Solution

Kamran Saifullah · Follow
4 min read · Aug 29, 2019

Listen Share

This is the last executable we need to analyze provided in the Labs for Chapter 1. Let's begin!

Let's analyze it via VirusTotal.



52 engines detected this file

0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126
Lab01-04.exe
armadillo peexe via-tor

36 KB Size

2019-05-23 22:30:51 UTC 19 days ago

Basic Properties

MD5	625ac05fd47adc3c63700c3b30de79ab
SHA-1	9369d80106dd245938996e245340a3c6f17587fe
SHA-256	0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126
Authentihash	e4d9d8ea008b5521c4b4273b8a276cf618db3f8af0bdd2f17d50f6c09e5bc150
Imphash	aade0ea6fbdcd9b8e96fe999cae6f603
SSDEEP	96:TF0MgAr71nxY9AAIvqZ2ZNHHsP4oynLKcm5OzG38U6p2WL4P4oyn:IJaPLjC2ZN
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	36 KB (36864 bytes)
PEiD	Armadillo v1.71

History

Creation Time	2019-08-30 22:26:59
First Seen In The Wild	2011-07-05 16:16:16
First Submission	2011-07-06 00:05:42
Last Submission	2019-05-23 22:30:51
Last Analysis	2019-05-23 22:30:51

Names

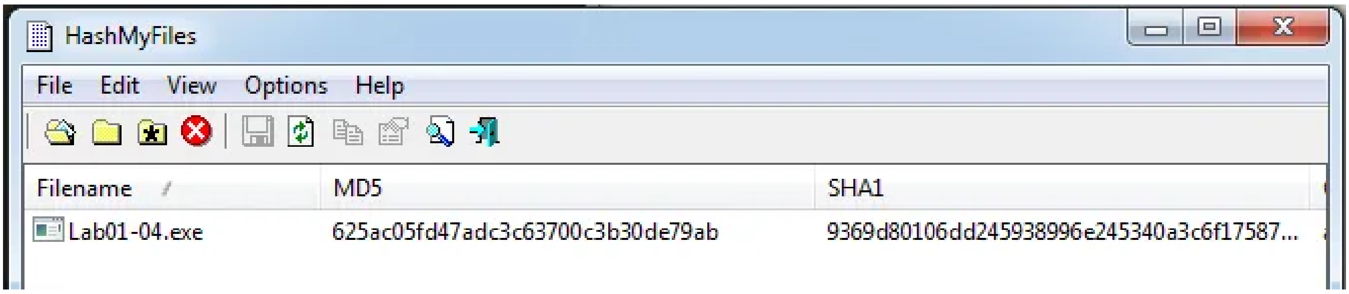
Lab01-04.exe
Laudo02.bin
sample4.exe
homework1.dat
homework1.exe
LabII_04.exe
HW1-1.ex_
malware.exe
malware6.exe
Lab01-04.vxe

Portable Executable Info

Header

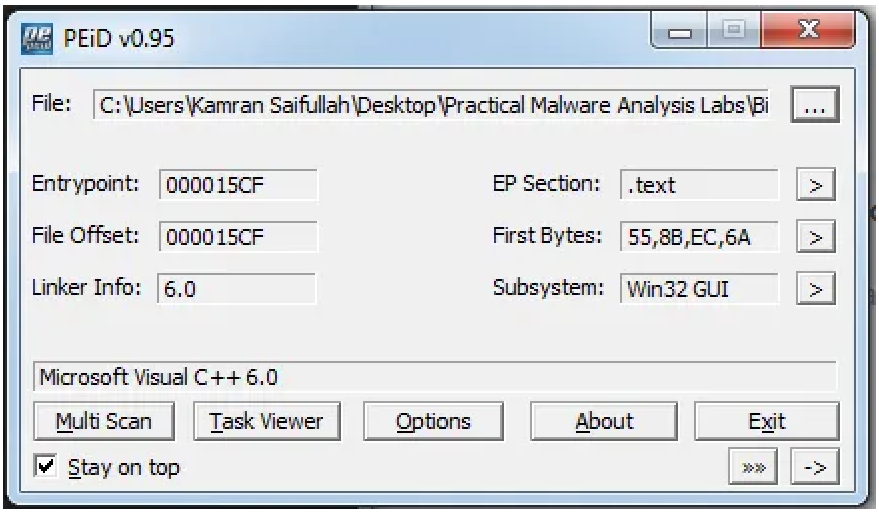
Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2019-08-30 22:26:59
Entry Point	5583
Contained Sections	4

Let's tally the hashes!



Filename	MD5	SHA1
Lab01-04.exe	625ac05fd47adc3c63700c3b30de79ab	9369d80106dd245938996e245340a3c6f17587...

The hashes are correct. Let's move onto checking whether this executable is packed or not.



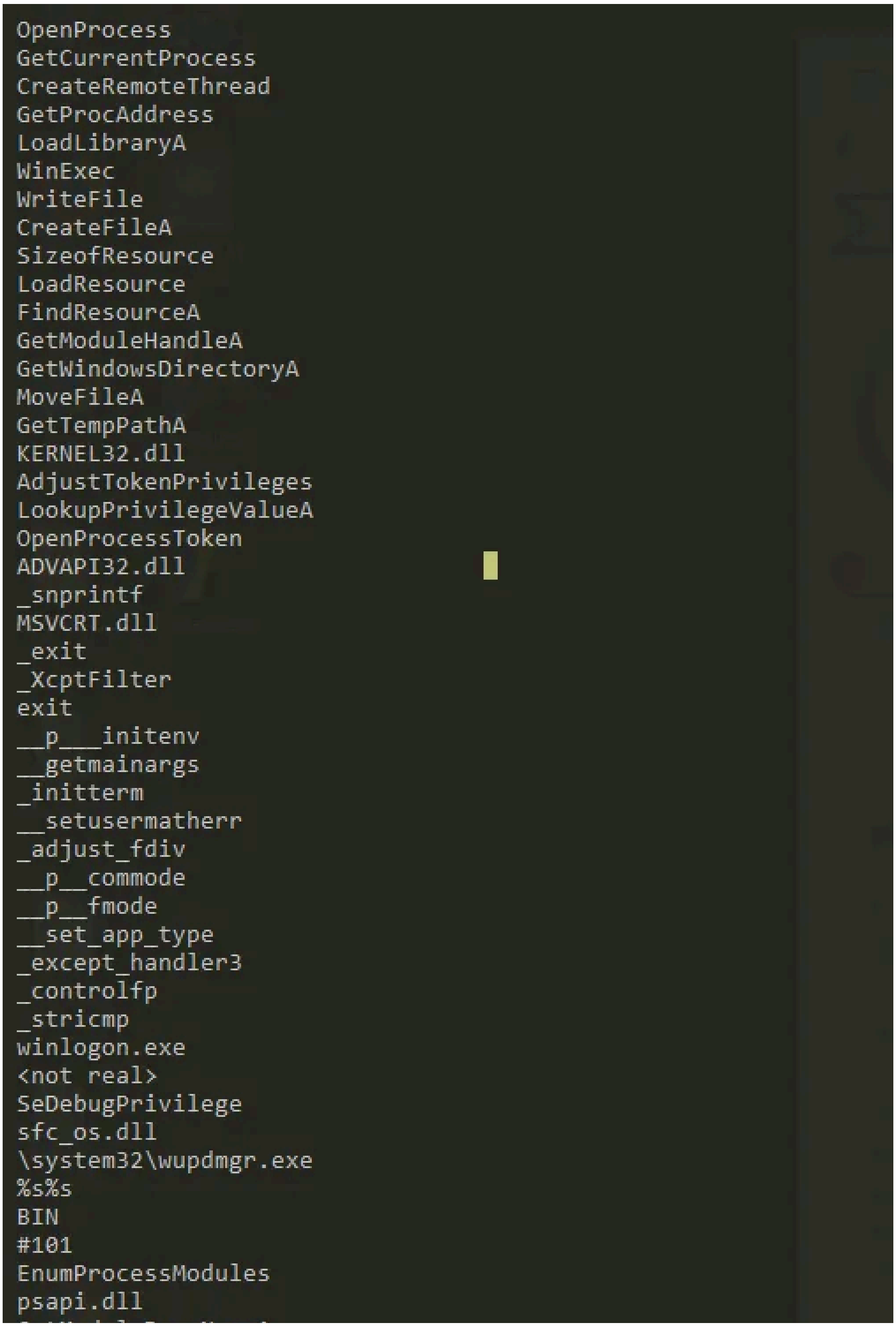
File: C:\Users\Kamran Saifullah\Desktop\Practical Malware Analysis Labs\Bi

Entrypoint: 000015CF
EP Section: .text
File Offset: 000015CF
First Bytes: 55,8B,EC,6A
Linker Info: 6.0
Subsystem: Win32 GUI

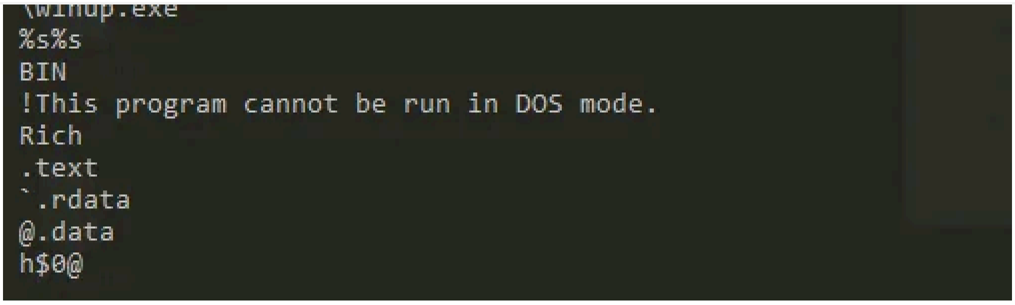
Microsoft Visual C++ 6.0

☑ Stay on top

This executable does not seems to be packed. Let's run the strings or you can use BinText (It's good) for locating the strings :))

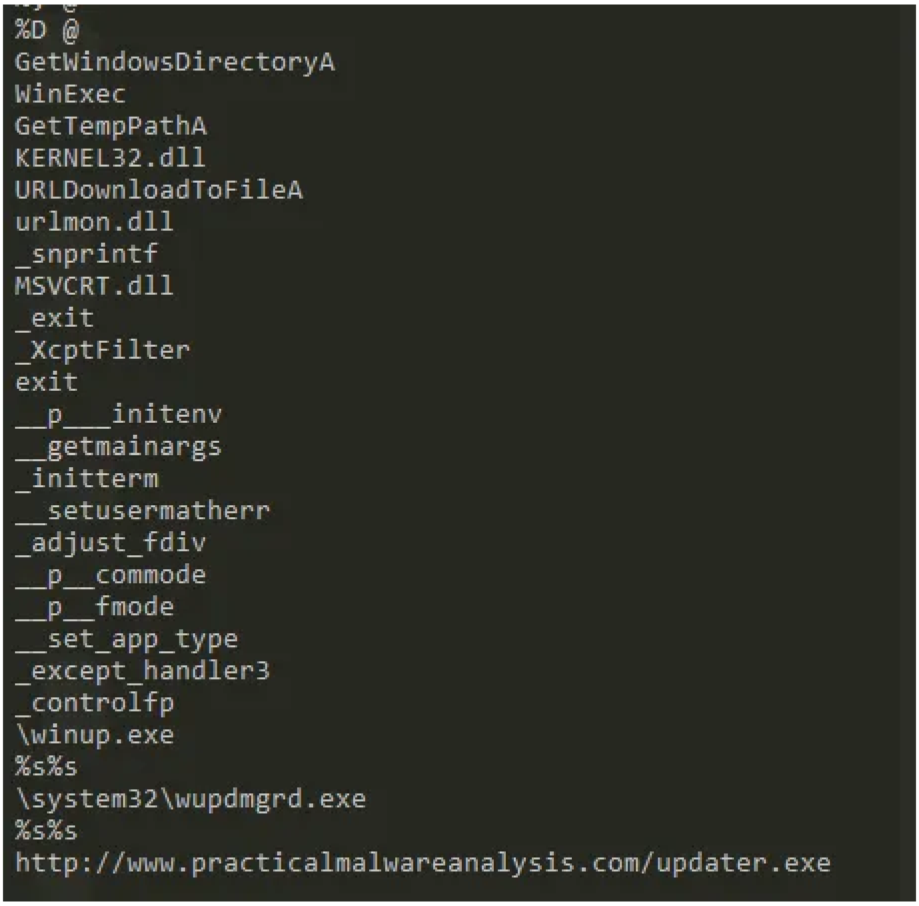


```
OpenProcess
GetCurrentProcess
CreateRemoteThread
GetProcAddress
LoadLibraryA
WinExec
WriteFile
CreateFileA
SizeofResource
LoadResource
FindResourceA
GetModuleHandleA
GetWindowsDirectoryA
MoveFileA
GetTempPathA
KERNEL32.dll
AdjustTokenPrivileges
LookupPrivilegeValueA
OpenProcessToken
ADVAPI32.dll
_snprintf
MSVCRT.dll
_exit
_XcptFilter
exit
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
_stricmp
winlogon.exe
<not real>
SeDebugPrivilege
sfc_os.dll
\system32\wupdmgr.exe
%s%s
BIN
#101
EnumProcessModules
psapi.dll
```



```
\winup.exe
%s%s
BIN
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
h$0@
```

We have quite a lot of information regarding the DLL and the functions which are being imported.

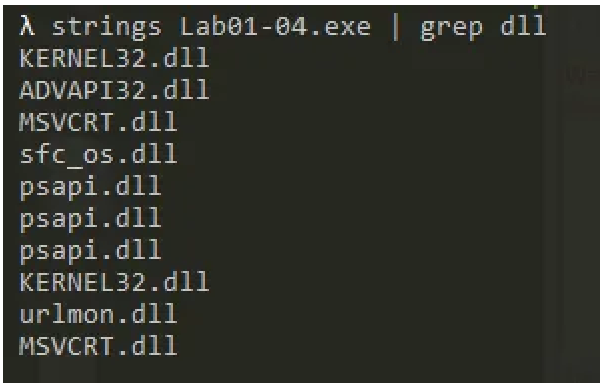


```
%D @
GetWindowsDirectoryA
WinExec
GetTempPathA
KERNEL32.dll
URLDownloadToFileA
urlmon.dll
_snprintf
MSVCRT.dll
_exit
_XcptFilter
exit
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
\winup.exe
%s%s
\system32\wupdmgrd.exe
%s%s
http://www.practicalmalwareanalysis.com/updater.exe
```

Also we can see that three more executables are being accessed and updater.exe is being downloaded from the URL. Let's take a closer look onto this using DependencyWalker.

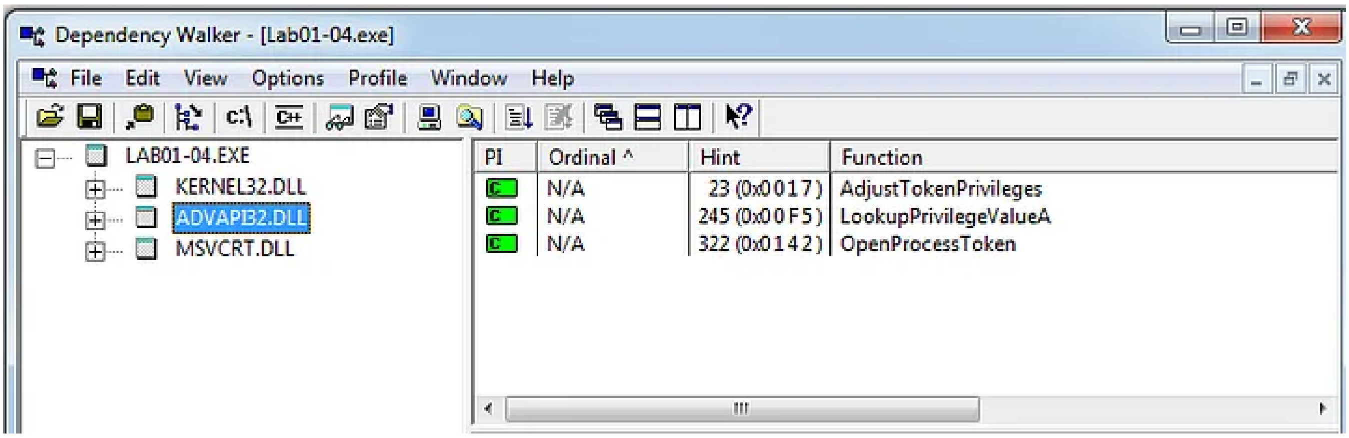
> ***NOTE:*** I personally like to perform a strings along with the grep command to reveal more information. Rather than directly going for the DependencyWalker. The reason? Below are the two screenshots!.

Why strings?



```
λ strings Lab01-04.exe | grep dll
KERNEL32.dll
ADVAPI32.dll
MSVCRT.dll
sfc_os.dll
psapi.dll
psapi.dll
psapi.dll
KERNEL32.dll
urlmon.dll
MSVCRT.dll
```

Why DependencyWalker?

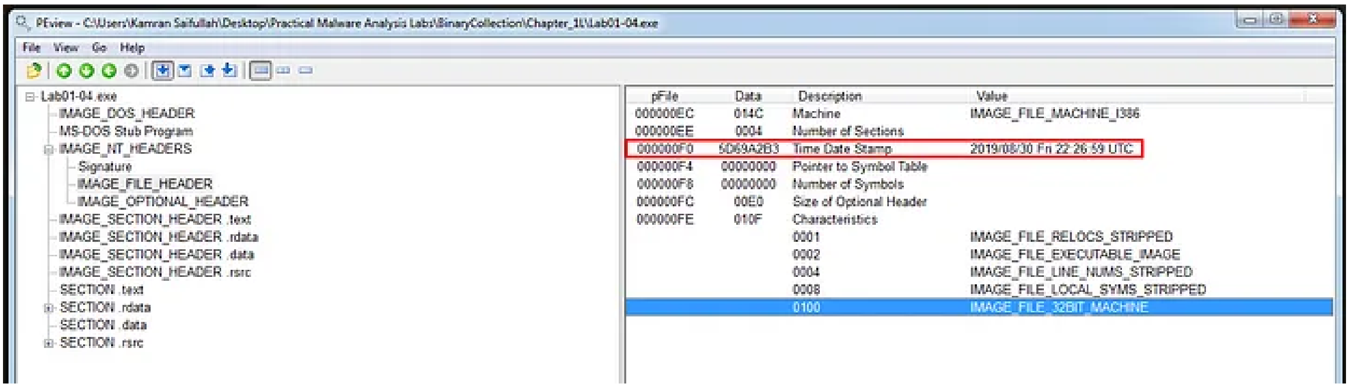


```
LAB01-04.EXE
    KERNEL32.DLL
    ADVAPI32.DLL
    MSVCRT.DLL
```

PI	Ordinal ^	Hint	Function
C	N/A	23 (0x0017)	AdjustTokenPrivileges
C	N/A	245 (0x00F5)	LookupPrivilegeValueA
C	N/A	322 (0x0142)	OpenProcessToken

I hope it’s clear now ;)

Let’s check the compilation time of this executable by using PEview.


PEview - C:\Users\Kamran Saifullah\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-04.exe
File
View
Go
Help

```
Lab01-04.exe
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
    IMAGE_NT_HEADERS
        Signature
        IMAGE_FILE_HEADER
        IMAGE_OPTIONAL_HEADER
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .rdata
    IMAGE_SECTION_HEADER .data
    IMAGE_SECTION_HEADER .rsrc
    SECTION .text
    SECTION .rdata
    SECTION .data
    SECTION .rsrc
```

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0004	Number of Sections	
000000F0	5D69A2B3	Time Date Stamp	2019/08/30 Fri 22:26:59 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE

We can clearly see that the compilation time is of FRI 30/08/2019.

Let’s look onto the important functionality of this executable.

LoadResource, **FindResource** and **SizeOfResource** are being used to load the data from the resource section.

GetWindowsDirectory is indicating that directories is being checked where the file maybe written to.

WinExec tells that the program is being executed.

CreateFile & **WriteFile** indicates that a file is being created and written.

AdjustTokenPrivileges function enables or disables privileges.

Moreover we can see that two more programs are being executed!

\winup.exe
\system32\wupdmgrd.exe

The updater is being downloaded from the website!
http://www.practicalmalwareanalysis.com/updater.exe

Let’s answer the questions now!

Lab 1–4

Analyze the file Lab01–04.exe

Questions

a. **Upload the Lab01–04.exe file to http://www.VirusTotal.com/. Does it match?**

We have uploaded the file and found it malicious.

b. **Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.**

The file is not packed at all.

c. **When was this program compiled?**

This program was compiled on 30/08/2019 but it doesn’t seems to be correct!

d. **Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you?**

Files are being created and written to. Also some other executable’s are being executed and updater is being download from the URL.

e. **What host- or network-based indicators could be used to identify this malware on infected machines?**

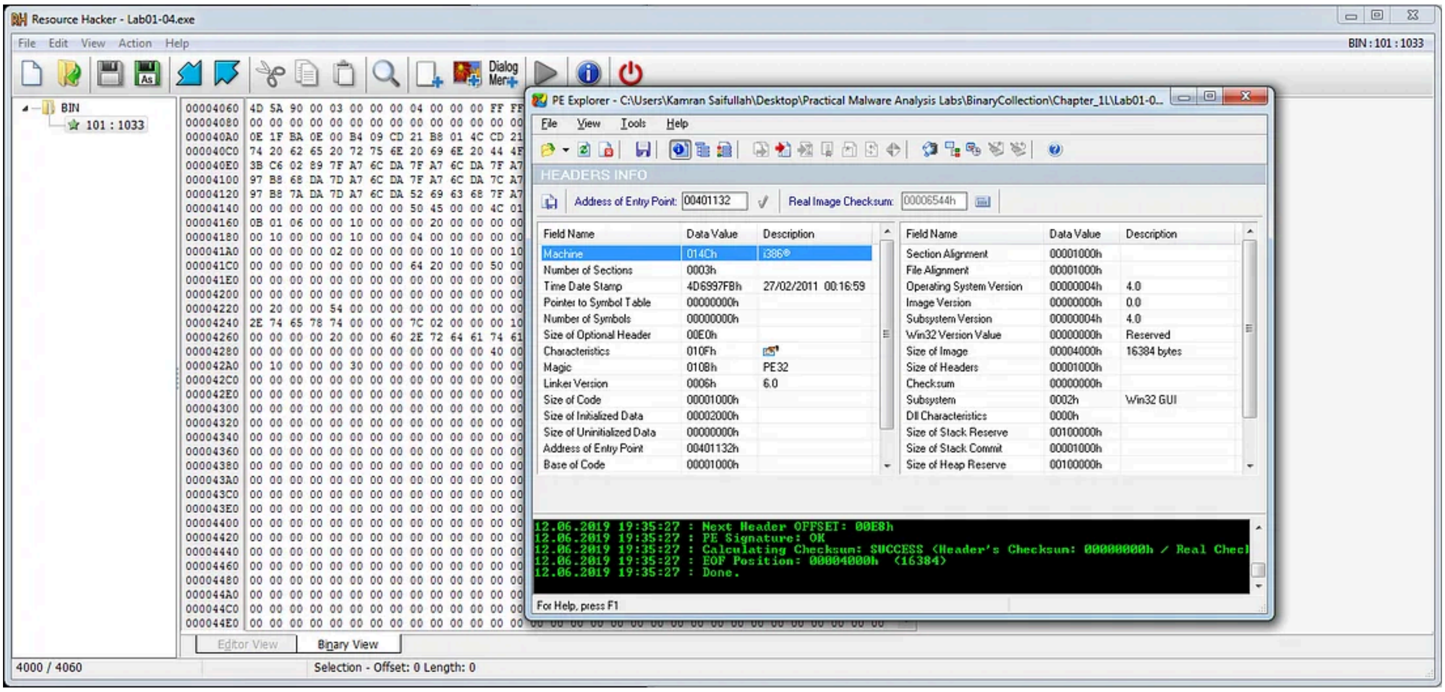
Host-Based

\winup.exe
\system32\wupdmgrd.exe

Network-Based
http://www.practicalmalwareanalysis.com/updater.exe

f. This file has one resource in the resource section. Use Resource Hacker to examine that resource, and then use it to extract the resource. What can you learn from the resource?

The part d and e are the answers of this part. But let’s use Resource Hacker as we haven’t tried it yet and try to extract the resource!


Resource Hacker - Lab01-04.exe
File Edit View Action Help
BIN : 101 : 1033
Dialog Mer
BIN
101 : 1033
PE Explorer - C:\Users\Kamran Saifullah\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L\Lab01-0...
File View Tools Help
HEADERS INFO
Editor View
Binary View
4000 / 4060
Selection - Offset: 0 Length: 0
For Help, press F1

```
00004060  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF
00004080  00 00 00 00 00 00 00 00 00 00 00 00 00 00
000040A0  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21
000040C0  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F
000040E0  3B C6 02 89 7F A7 6C DA 7F A7 6C DA 7F A7
00004100  97 B8 68 DA 7D A7 6C DA 7F A7 6C DA 7C A7
00004120  97 B8 7A DA 7D A7 6C DA 52 69 63 68 7F A7
00004140  00 00 00 00 00 00 00 00 50 45 00 00 4C 01
00004160  0B 01 06 00 00 10 00 00 00 20 00 00 00 00
00004180  00 10 00 00 00 10 00 00 04 00 00 00 00 00
000041A0  00 00 00 00 02 00 00 00 00 00 10 00 00 10
000041C0  00 00 00 00 00 00 00 00 64 20 00 00 50 00
000041E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004200  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004220  00 20 00 00 54 00 00 00 00 00 00 00 00 00
00004240  2E 74 65 78 74 00 00 00 7C 02 00 00 00 10
00004260  00 00 00 00 20 00 00 60 2E 72 64 61 74 61
00004280  00 00 00 00 00 00 00 00 00 00 00 00 40 00
000042A0  00 10 00 00 00 30 00 00 00 00 00 00 00 00
000042C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00
000042E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004300  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004320  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004340  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004360  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004380  00 00 00 00 00 00 00 00 00 00 00 00 00 00
000043A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00
000043C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00
000043E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004400  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004420  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004440  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004460  00 00 00 00 00 00 00 00 00 00 00 00 00 00
00004480  00 00 00 00 00 00 00 00 00 00 00 00 00 00
000044A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00
000044C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00
000044E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Address of Entry Point: 00401132 Real Image Checksum: 00006544h

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0003h	
Time Date Stamp	4D6997FBh	27/02/2011 00:16:59
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	010Fh	
Magic	010Bh	PE32
Linker Version	0006h	6.0
Size of Code	00001000h	
Size of Initialized Data	00002000h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	00401132h	
Base of Code	00001000h	

Field Name	Data Value	Description
Section Alignment	00001000h	
File Alignment	00001000h	
Operating System Version	00000004h	4.0
Image Version	00000000h	0.0
Subsystem Version	00000004h	4.0
Win32 Version Value	00000000h	Reserved
Size of Image	00004000h	16384 bytes
Size of Headers	00001000h	
Checksum	00000000h	
Subsystem	0002h	Win32 GUI
Dll Characteristics	0000h	
Size of Stack Reserve	00100000h	
Size of Stack Commit	00001000h	
Size of Heap Reserve	00100000h	

```
12.06.2019 19:35:27 : Next Header OFFSET: 00E8h
12.06.2019 19:35:27 : PE Signature: OK
12.06.2019 19:35:27 : Calculating Checksum: SUCCESS (Header's Checksum: 00000000h / Real Chec
12.06.2019 19:35:27 : EOF Position: 00004000h  (16384)
12.06.2019 19:35:27 : Done.
```

We can finally save the resource as .bin and load in into PE-Explorer where we can see the compilation time of this resource to be 27/02/2011 :))

That’s all! We are done with Chapter-1. I hope that you have enjoyed :))

Thank You

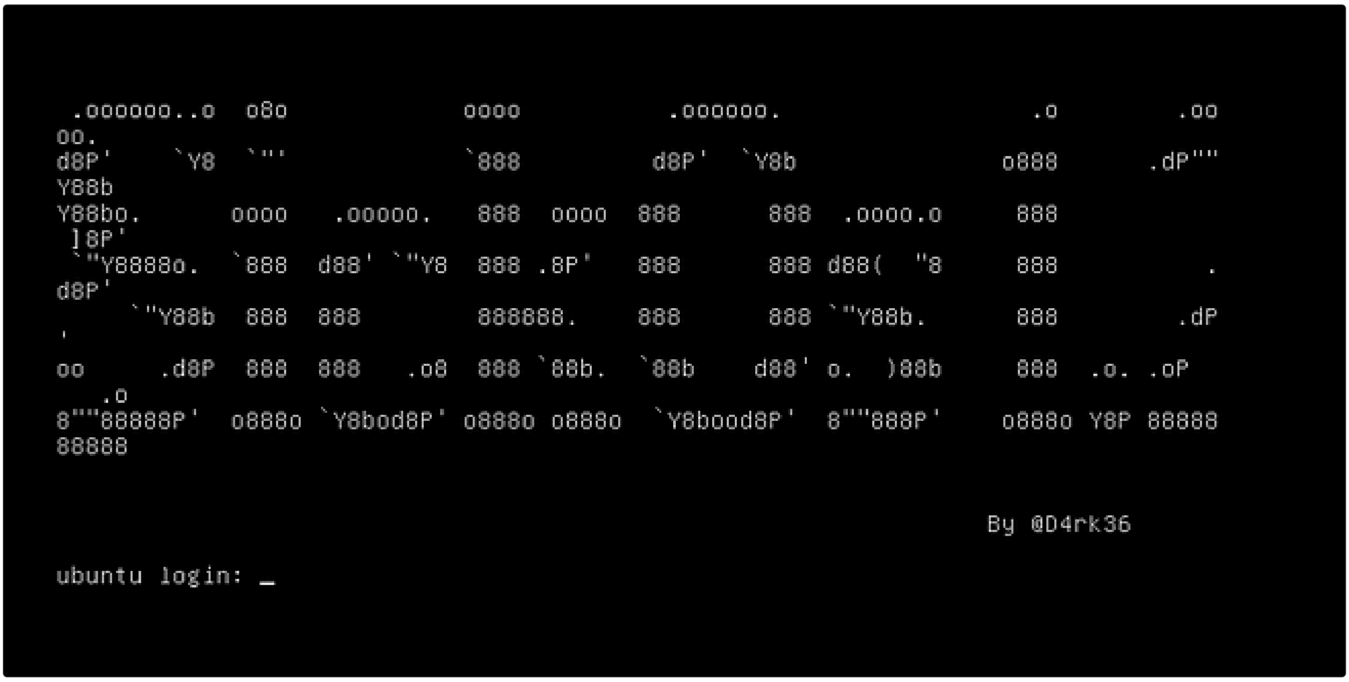
Follow

Written by Kamran Saifullah

378 Followers

Malware/RE/Firmware Analysis, App Sec/Off Sec, VAPT, Phishing Simulations/SE | Risk Management, IS Governance, Audits, ISO 27001 LI

More from Kamran Saifullah



```
 .oooooo..o  o8o            oooo          .oooooo.                 .o       .oo
oo.
d8P'    `Y8  `"'            `888         d8P'  `Y8b              o888      .dP""
Y88b
Y88bo.      oooo   .ooooo.   888  oooo  888      888  .oooo.o     888
 ]8P'
 `"Y8888o.  `888  d88' `"Y8  888 .8P'   888      888 d88(  "8     888          .
d8P'
     `"Y88b  888  888        888888.    888      888 `"Y88b.      888        .dP
'
oo     .d8P  888  888   .o8  888 `88b.  `88b    d88' o.  )88b     888  .o. .oP
   .o
8""88888P'  o888o `Y8bod8P' o888o o888o  `Y8bood8P'  8""888P'    o888o Y8P 88888
88888


                                                                By @D4rk36

ubuntu login: _
```

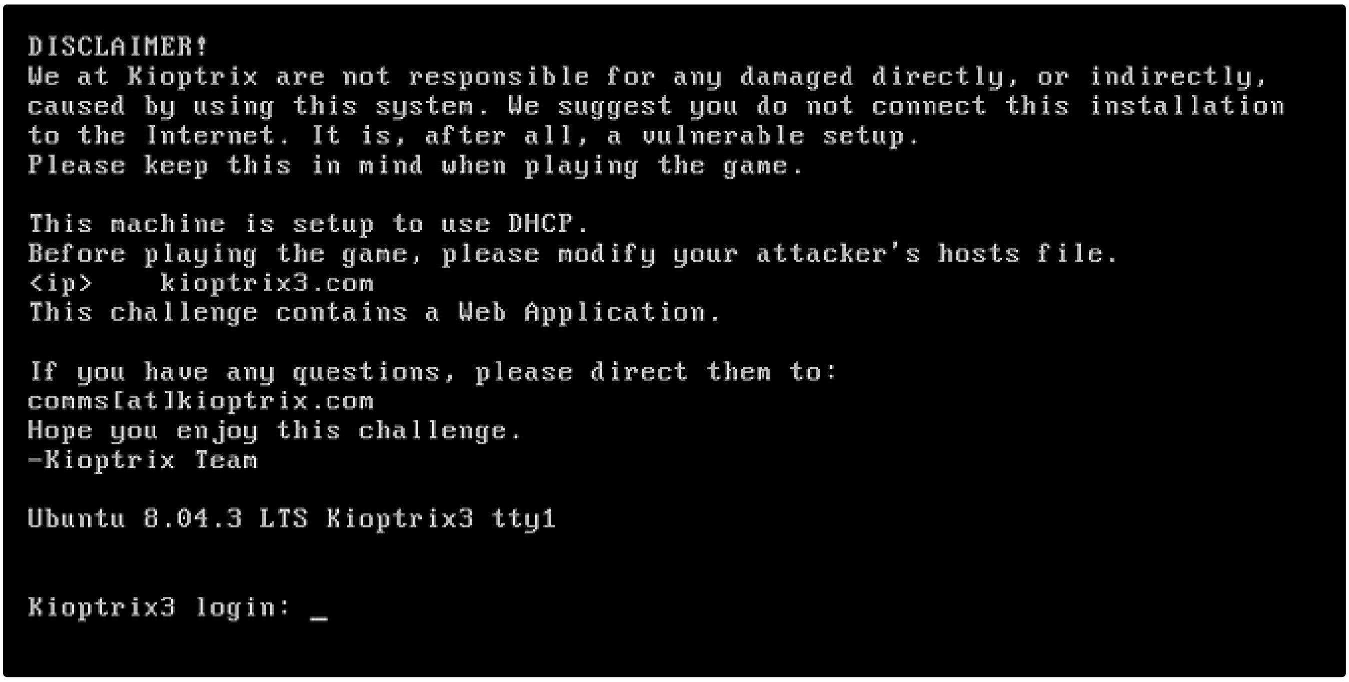
Kamran Saifullah

SickOS 1.2 WalkThrough

Hi,

5 min read · Apr 14, 2018

10



```
DISCLAIMER!
We at Kioptrix are not responsible for any damaged directly, or indirectly,
caused by using this system. We suggest you do not connect this installation
to the Internet. It is, after all, a vulnerable setup.
Please keep this in mind when playing the game.

This machine is setup to use DHCP.
Before playing the game, please modify your attacker's hosts file.
<ip>    kioptrix3.com
This challenge contains a Web Application.

If you have any questions, please direct them to:
comms[at]kioptrix.com
Hope you enjoy this challenge.
-Kioptrix Team

Ubuntu 8.04.3 LTS Kioptrix3 tty1


Kioptrix3 login: _
```

Kamran Saifullah

WalkThrough! Kioptrix — 3 By VulnHub

Hi,

8 min read · Mar 13, 2018

24

52

Written by: Jeremy Hui

Keith is watching chickens cross a road in his grandfather's farm. He once heard from his grandfather that there was something significant about this behavior, but he can't figure out why. Help Keith discover what the chickens are doing from this seemingly simple behavior.

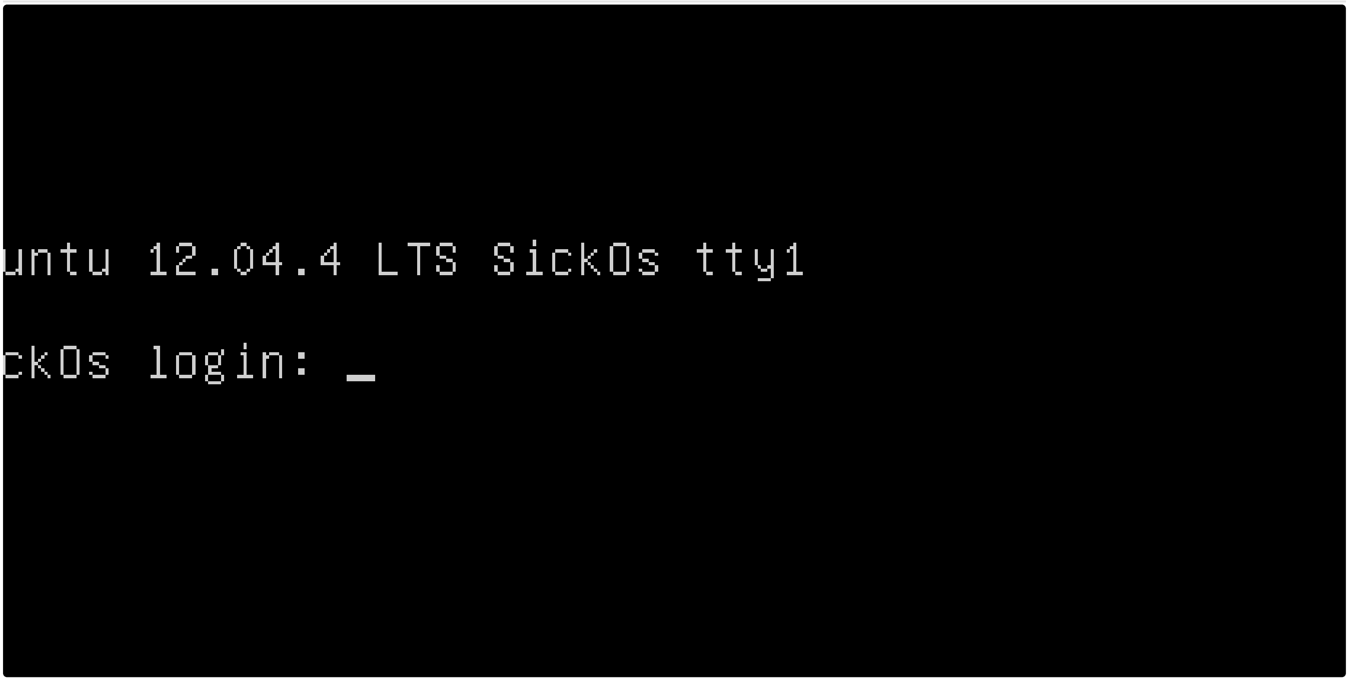
Kamran Saifullah

HSCTF 6—Forensics Challenges—Solutions

After publishing the solutions of the web challenges now it's time to move on with forensics challenges and this is all about how i solved...

5 min read · Jun 13, 2019

17



```
untu 12.04.4 LTS SickOs tty1

ckOs login: _
```

Kamran Saifullah

SickOS 1.1 Walkthrough

Hi,

5 min read · Apr 11, 2018

9

See all from Kamran Saifullah

Recommended from Medium

Abdelwahab Shandy

CyberDefenders :Qradar101 Blue Team Challenge

Category : Threat Hunting

11 min read · Nov 23, 2023

4

Worldsleaks

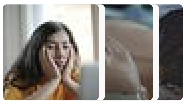
OpenWire—

CyberDefenders CTF

7 min read · Jan 25, 2024

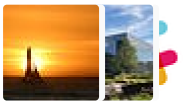
13

Lists



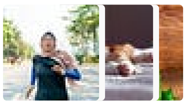
Staff Picks

630 stories · 920 saves



Stories to Help You Level-Up at Work

19 stories · 581 saves

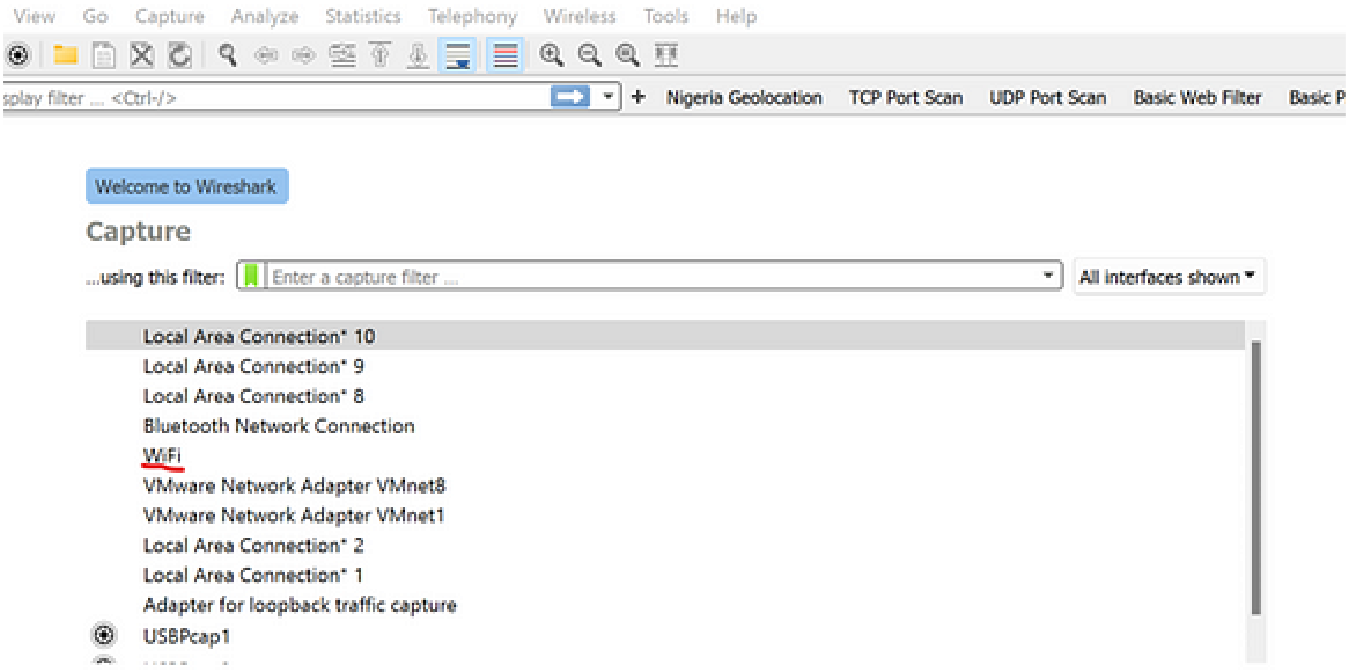


Self-Improvement 101

20 stories · 1675 saves

Productivity 101

20 stories · 1543 saves



Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
WiFi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 2
Local Area Connection* 1
Adapter for loopback traffic capture
USBPcap1

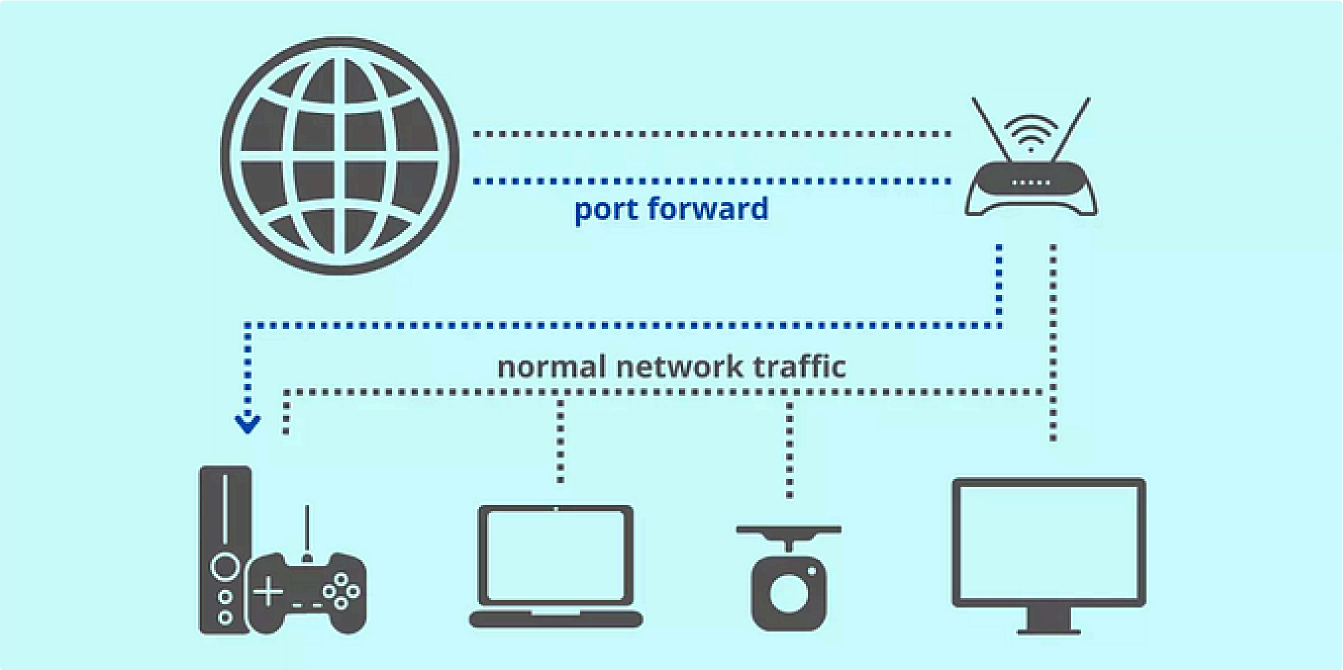
Kevin Moore

Analyzing PCAP Files using Wireshark

Hello, thanks for stopping by to read this blog. Its a deep-dive into the use of Wireshark to investigate captured network traffic.

6 min read · Nov 20, 2023

7



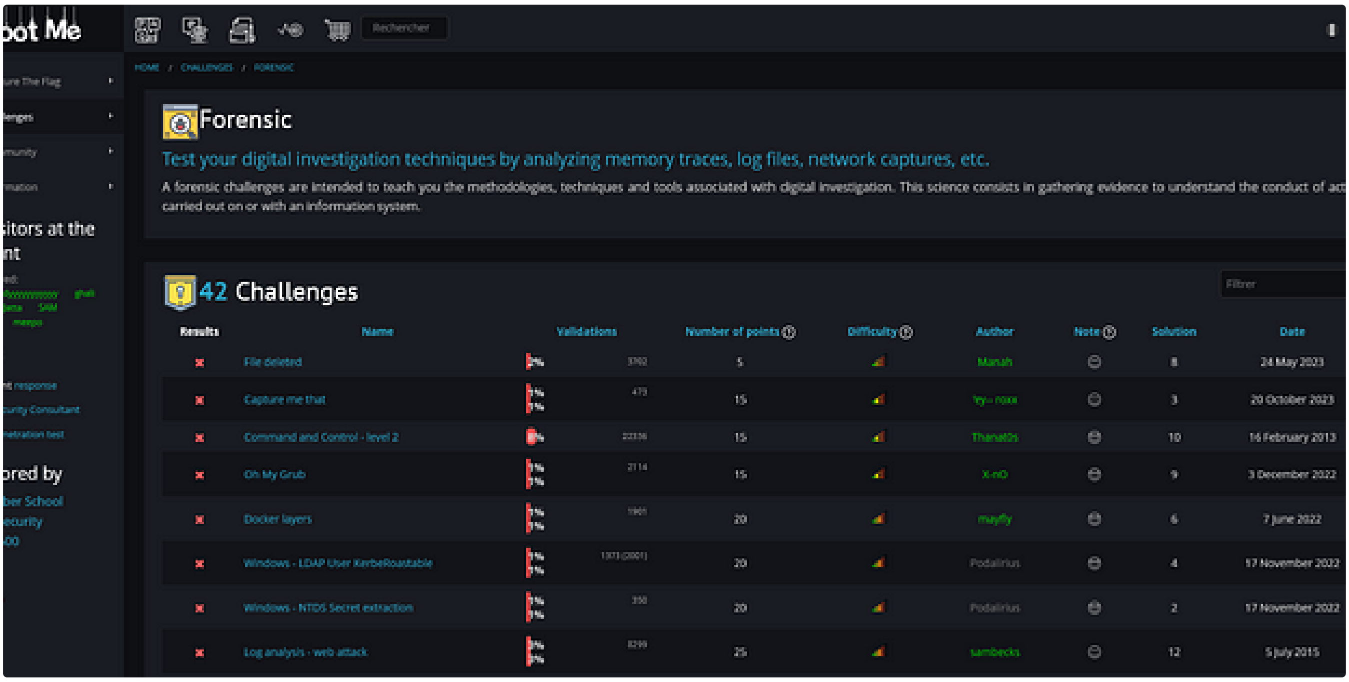
Subhajit Dutta

Demystifying Port Forwarding: A Comprehensive Guide

Navigating the Network Maze: Unveiling the Secrets of Port Forwarding, Secure Tunnels, and Power of OSI Layer 4

6 min read · Feb 18, 2024

9



Forensic

Test your digital investigation techniques by analyzing memory traces, log files, network captures, etc.

A forensic challenges are intended to teach you the methodologies, techniques and tools associated with digital investigation. This science consists in gathering evidence to understand the conduct of act carried out on or with an information system.

42 Challenges

Results	Name	Validations	Number of points	Difficulty	Author	Note	Solution	Date
✗	File deleted	3792	5		Manah	☺	8	24 May 2023
✗	Capture me that	473	15		'ey-- roxx	☺	3	20 October 2023
✗	Command and Control - level 2	22336	15		Thanat0s	☺	10	16 February 2013
✗	Oh My Grub	2114	15		X-n0	☺	9	3 December 2022
✗	Docker layers	1901	20		mayfly	☺	6	7 June 2022
✗	Windows - LDAP User KerbeRoastable	1373 (2001)	20		Podalirius	☺	4	17 November 2022
✗	Windows - NTDS Secret extraction	350	20		Podalirius	☺	2	17 November 2022
✗	Log analysis - web attack	8299	25		sambecks	☺	12	5 July 2015

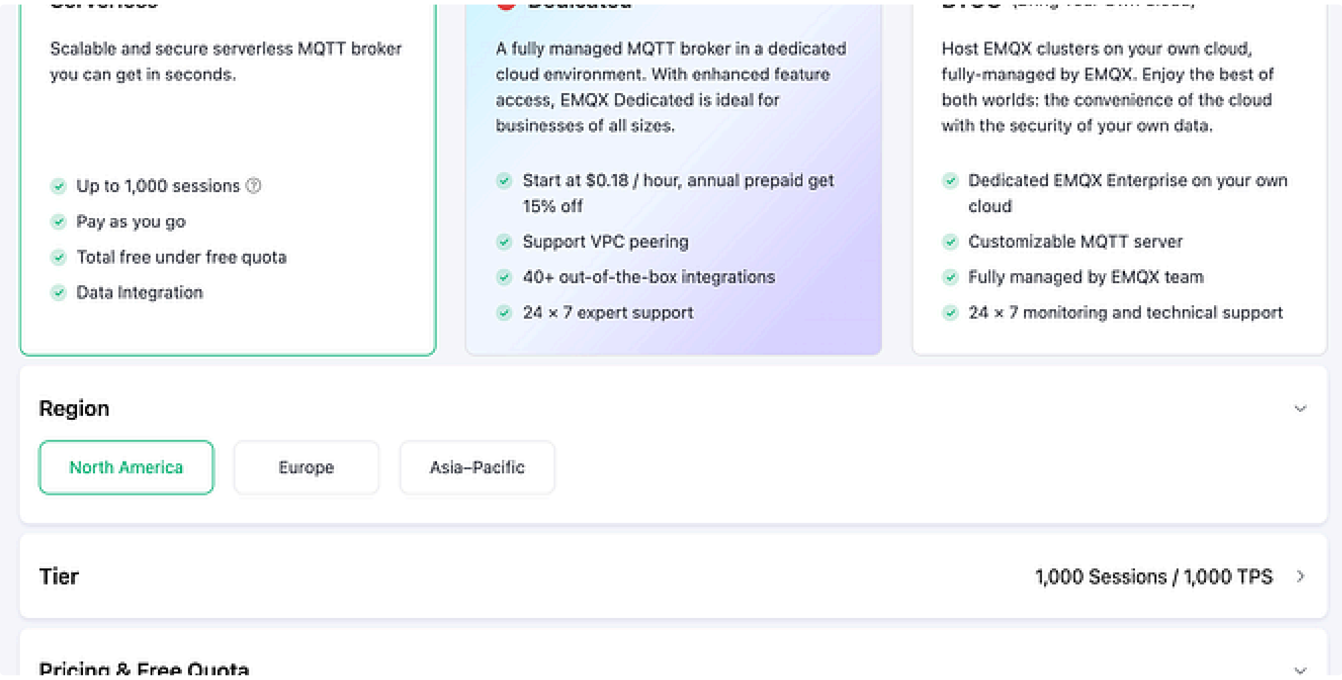
Jayvin Gohel

Root Me : File Deleted

Category : Forensic

4 min read · Jan 14, 2024

13



Scalable and secure serverless MQTT broker you can get in seconds.

- Up to 1,000 sessions
- Pay as you go
- Total free under free quota
- Data Integration

A fully managed MQTT broker in a dedicated cloud environment. With enhanced feature access, EMQX Dedicated is ideal for businesses of all sizes.

- Start at $0.18 / hour, annual prepaid get 15% off
- Support VPC peering
- 40+ out-of-the-box integrations
- 24 × 7 expert support

Host EMQX clusters on your own cloud, fully-managed by EMQX. Enjoy the best of both worlds: the convenience of the cloud with the security of your own data.

- Dedicated EMQX Enterprise on your own cloud
- Customizable MQTT server
- Fully managed by EMQX team
- 24 × 7 monitoring and technical support

Region

North America Europe Asia-Pacific

Tier 1,000 Sessions / 1,000 TPS

Pricing & Free Quota

EMQ Technologies

MQTT with openHAB: A Step-by-Step Tutorial

Introduction

6 min read · Apr 19, 2024

66

See more recommendations