Practical Malware Analysis — Chapter 1 — Lab 1–3 — Solution

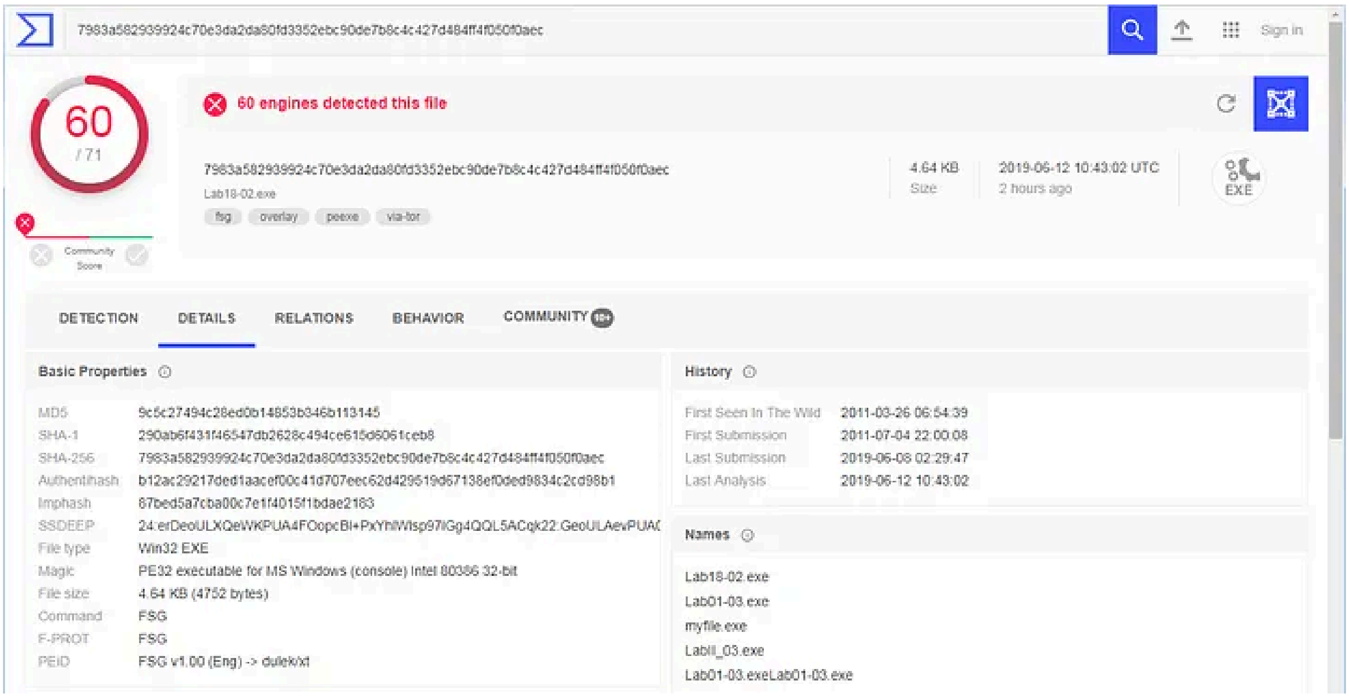
Kamran Saifullah · Follow

2 min read · Aug 29, 2019

Listen Share

By now we have successfully done analyzing two executable’s by using basic static analysis techniques. Now we have to analyze the third executable. Technique is the same. All we are doing is to polish our learning skills that we have learnt so far.

Let’s analyze it via VirusTotal.



7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec

60 / 71

60 engines detected this file

7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec
Lab18-02.exe
fsg overlay peexe via-tor

4.64 KB
Size

2019-06-12 10:43:02 UTC
2 hours ago

EXE

Basic Properties

MD5	9c5c27494c28ed0b14853b346b113145
SHA-1	290ab6f431f46547db2628c494ce615d6061ceb8
SHA-256	7983a582939924c70e3da2da80fd3352ebc90de7b8c4c427d484ff4f050f0aec
Authentihash	b12ac29217ded1aacef00c41d707eec62d429519d67138ef0ded9834c2cd98b1
Imphash	87bed5a7cba00c7e1f4015f1bdae2183
SSDEEP	24:erDeoULXQeWKPUA4FOopcBl+PxYhlWlsp97lGg4QQL5ACqk22:GeoULAevPUA(
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
File size	4.64 KB (4752 bytes)
Command	FSG
F-PROT	FSG
PEID	FSG v1.00 (Eng) -> dulek/xt

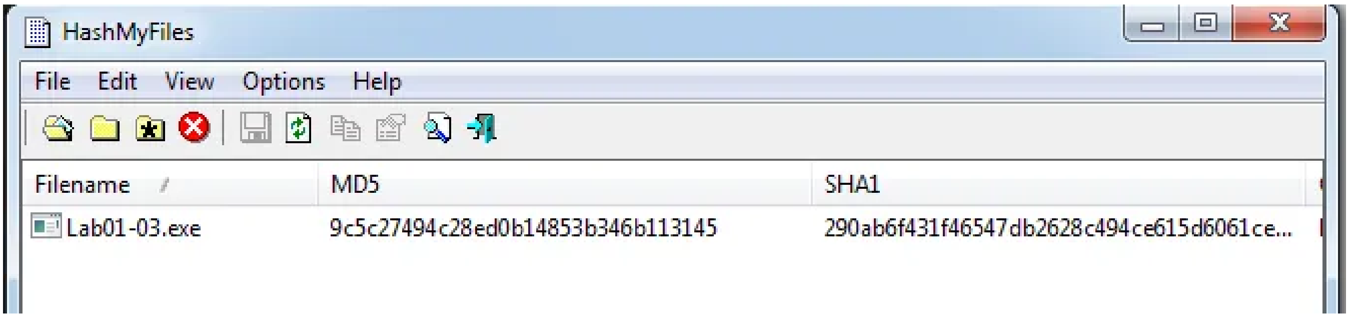
History

First Seen In The Wild	2011-03-26 06:54:39
First Submission	2011-07-04 22:00:08
Last Submission	2019-06-08 02:29:47
Last Analysis	2019-06-12 10:43:02

Names

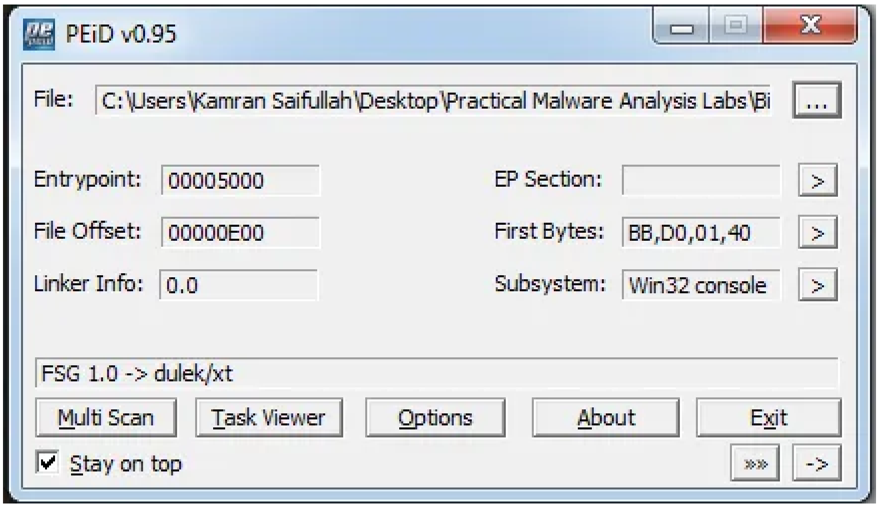
Lab18-02.exe
Lab01-03.exe
myfile.exe
Labll_03.exe
Lab01-03.exeLab01-03.exe

The file is malicious. Let’s create the fingerprint on our system.



Filename	MD5	SHA1
Lab01-03.exe	9c5c27494c28ed0b14853b346b113145	290ab6f431f46547db2628c494ce615d6061ce...

The hashes are same. Now, we need to check whether this file is packed or not!

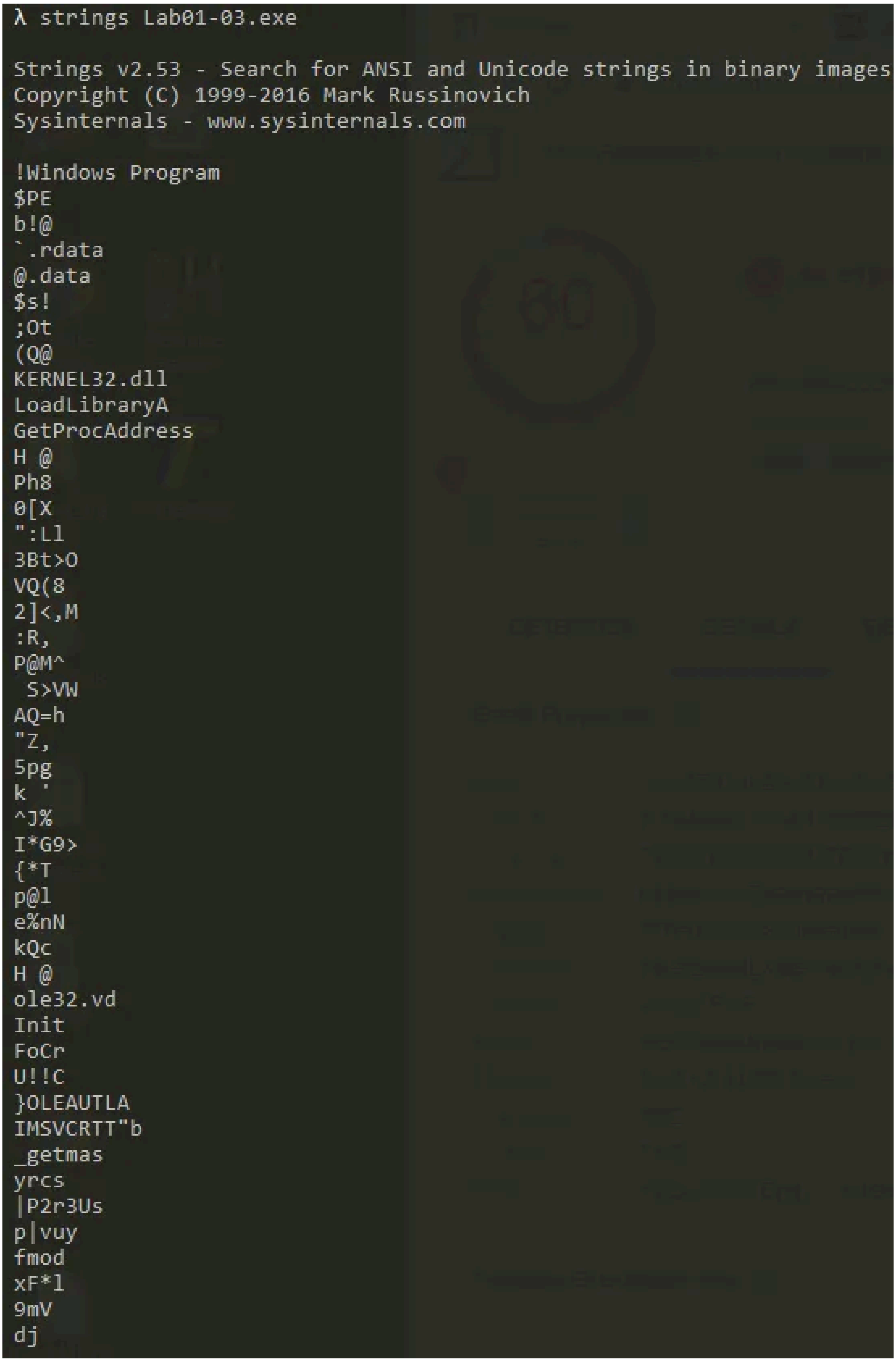


File: C:\Users\Kamran Saifullah\Desktop\Practical Malware Analysis Labs\Bi

Entrypoint: 00005000
EP Section:
File Offset: 00000E00
First Bytes: BB,D0,01,40
Linker Info: 0.0
Subsystem: Win32 console

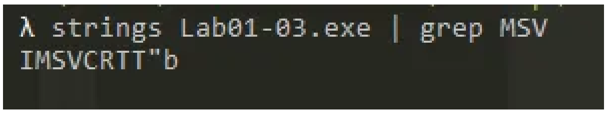
FSG 1.0 -> dulek/xt

The executable is packed using FSG 1.0, lets try to run strings on the executable and check if we are able to find any clue about this executable.



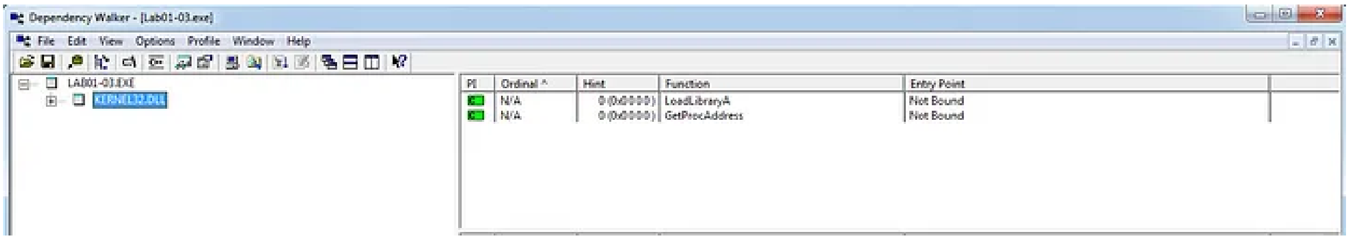
```
λ strings Lab01-03.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!Windows Program
$PE
b!@
`.rdata
@.data
$s!
;Ot
(Q@
KERNEL32.dll
LoadLibraryA
GetProcAddress
H @
Ph8
0[X
":Ll
3Bt>O
VQ(8
2]<,M
:R,
P@M^
 S>VW
AQ=h
"Z,
5pg
k '
^J%
I*G9>
{*T
p@l
e%nN
kQc
H @
ole32.vd
Init
FoCr
U!!C
}OLEAUTLA
IMSVCRTT"b
_getmas
yrcs
|P2r3Us
p|vuy
fmod
xF*l
9mV
dj
```

We can see the function 'LoadLibraryA, GetProcAddress" this proves that this file is packed. We also found the KERNEL32.DLL also MSVCRT.DLL as well!



```
λ strings Lab01-03.exe | grep MSV
IMSVCRTT"b
```

We don’t have any clue about the functions being imported. Let’s run the dependency walker to have a clue.


Dependency Walker - [Lab01-03.exe]
File Edit View Options Profile Window Help
LAB01-03.EXE
KERNEL32.DLL

PI	Ordinal ^	Hint	Function	Entry Point
🟩	N/A	0 (0x0000)	LoadLibraryA	Not Bound
🟩	N/A	0 (0x0000)	GetProcAddress	Not Bound

So we only have this information. Obviously this is not enough!

> ***NOTE:*** Leaving this Lab here as we will have to manually unpack this executable. We will work on this when we will learn about unpacking the executable at the end of the book.

Programming

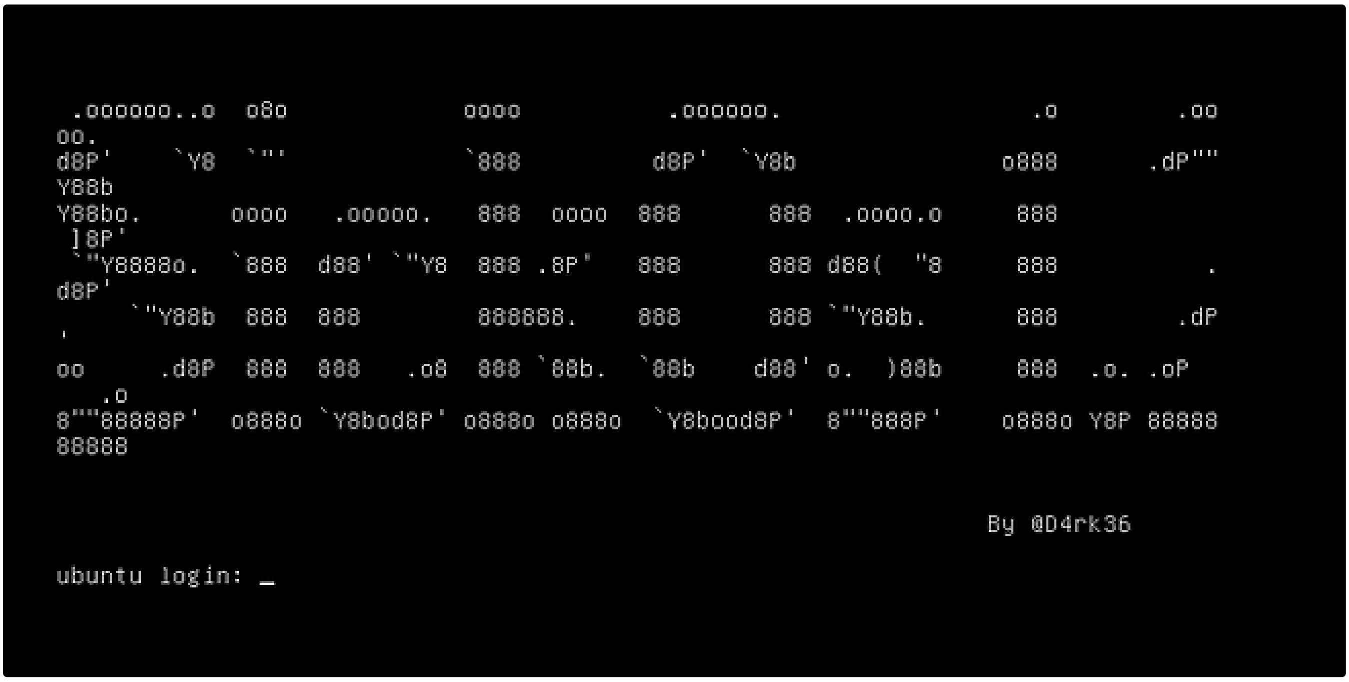
Follow

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: _
```

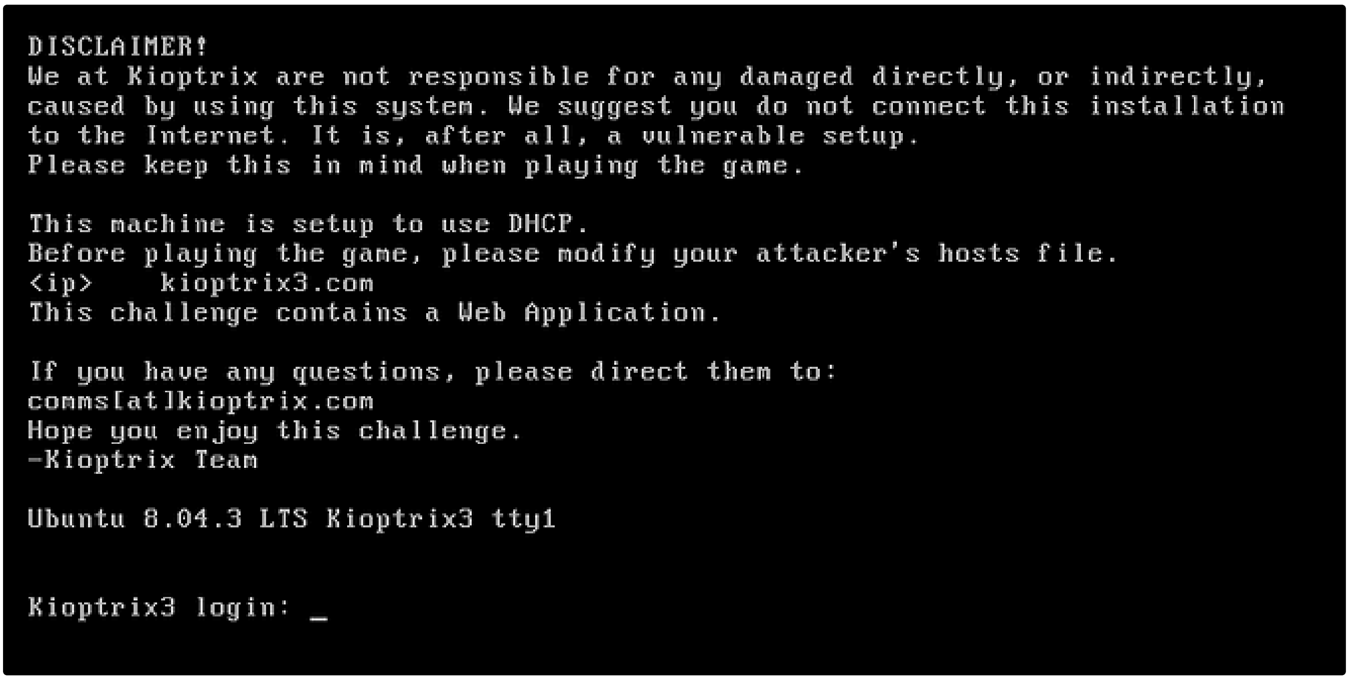
Kamran Saifullah

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: _
```

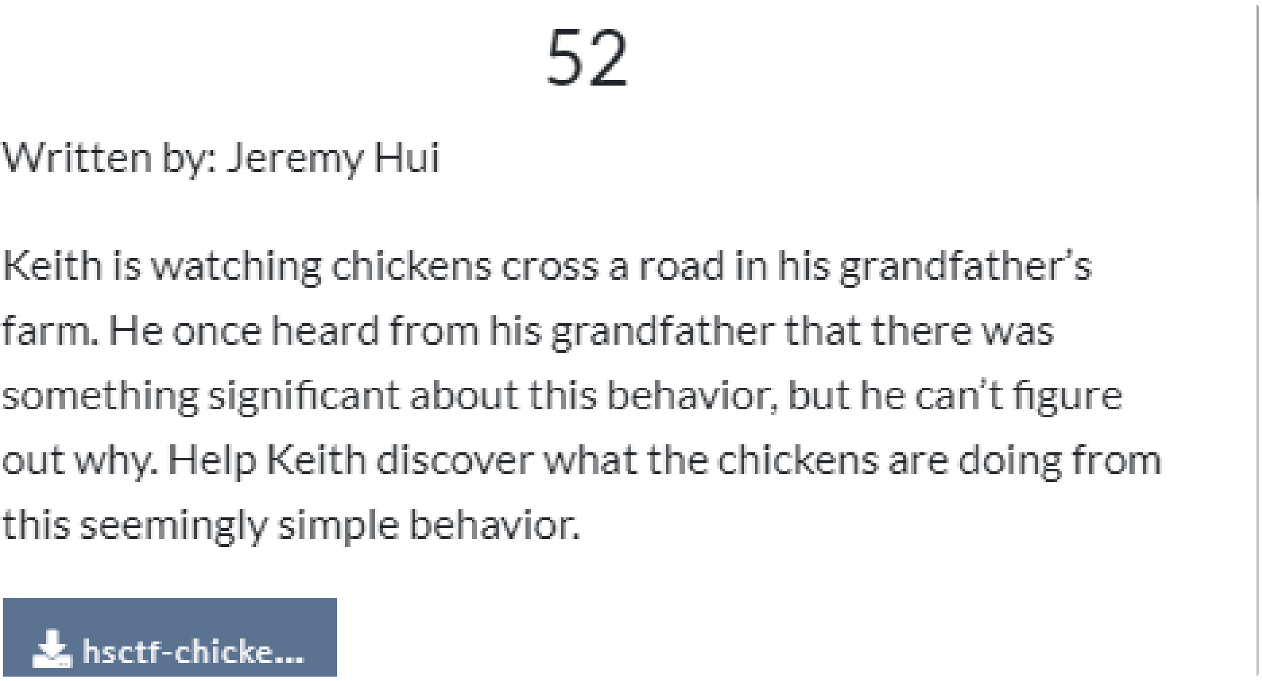
Kamran Saifullah

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.

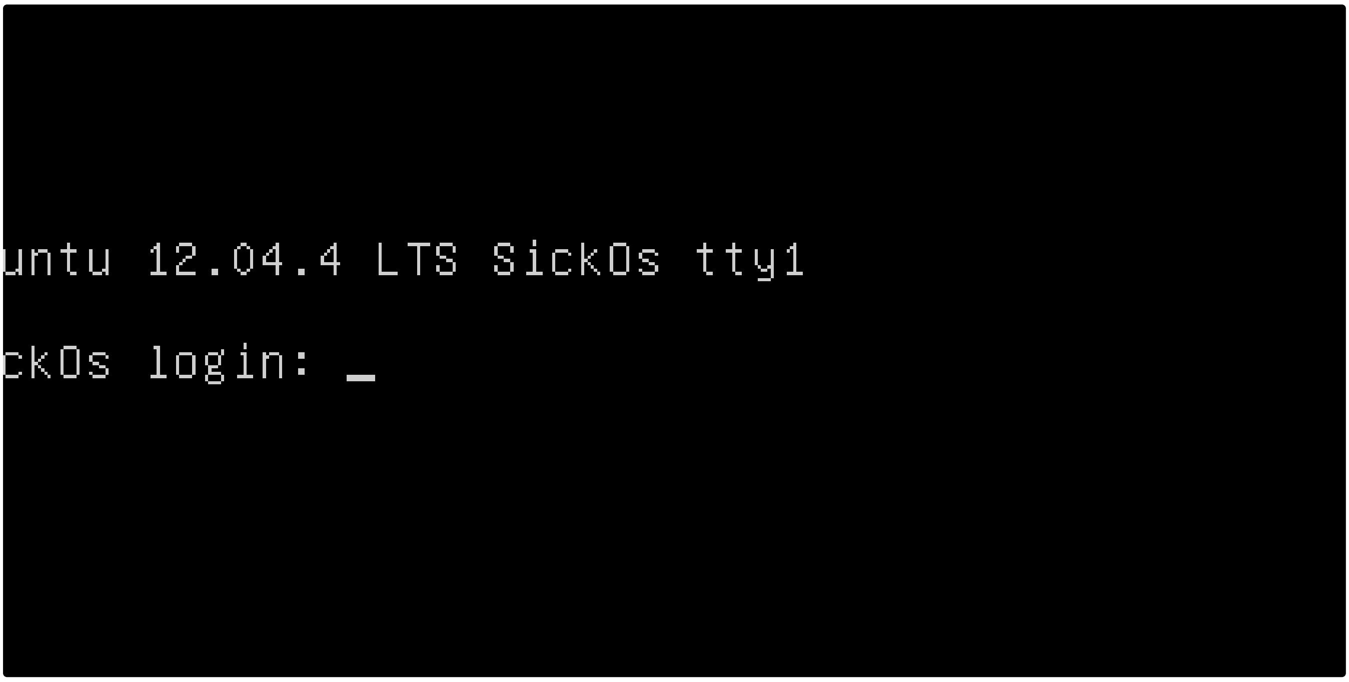
Kamran Saifullah

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

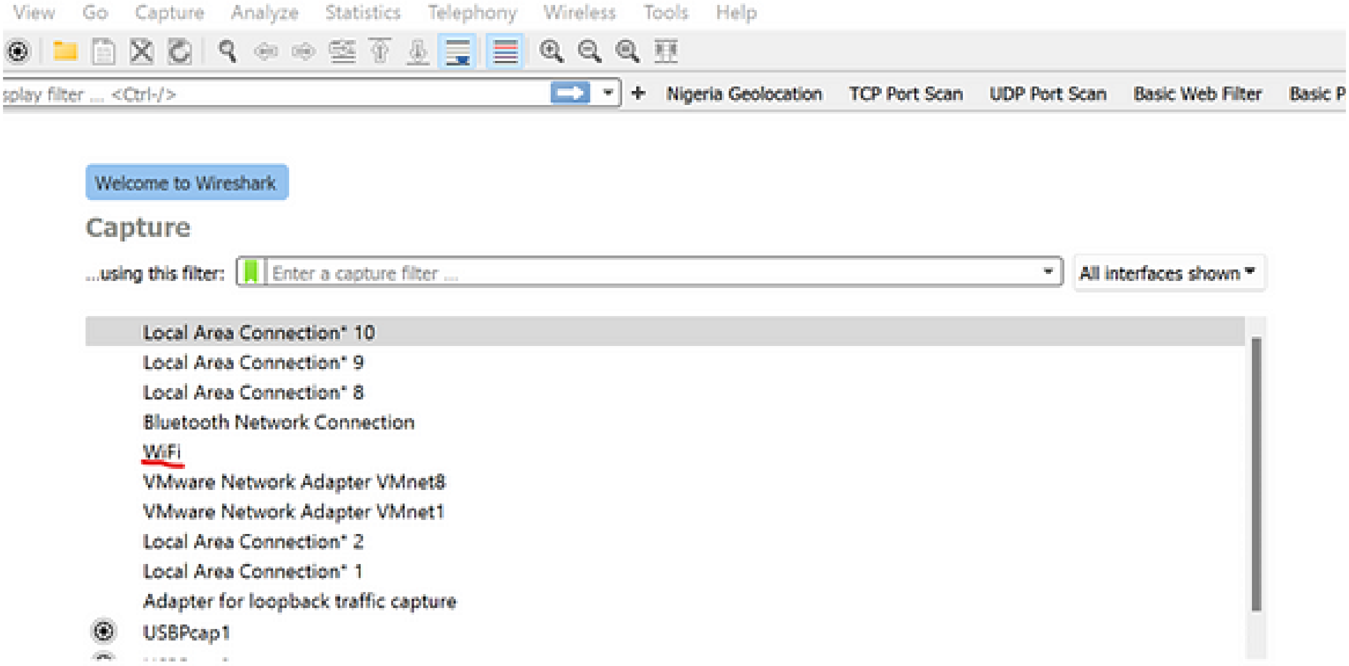
Hi,

5 min read · Apr 11, 2018

9

See all from Kamran Saifullah

Recommended from Medium


View Go Capture Analyze Statistics Telephony Wireless Tools Help
splay filter ... <Ctrl-/>
Nigeria Geolocation
TCP Port Scan
UDP Port Scan
Basic Web Filter
Basic P
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
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

Abhay Kumar

OOPs in Python

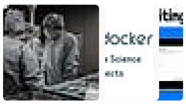
An easy guide

10 min read · Apr 9, 2024

Lists

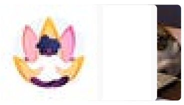
General Coding Knowledge

20 stories · 1148 saves



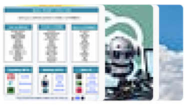
Coding & Development

11 stories · 579 saves



Stories to Help You Grow as a Software Developer

19 stories · 1007 saves



ChatGPT

21 stories · 596 saves

Worldsleaks

OpenWire—

CyberDefenders CTF

7 min read · Jan 25, 2024

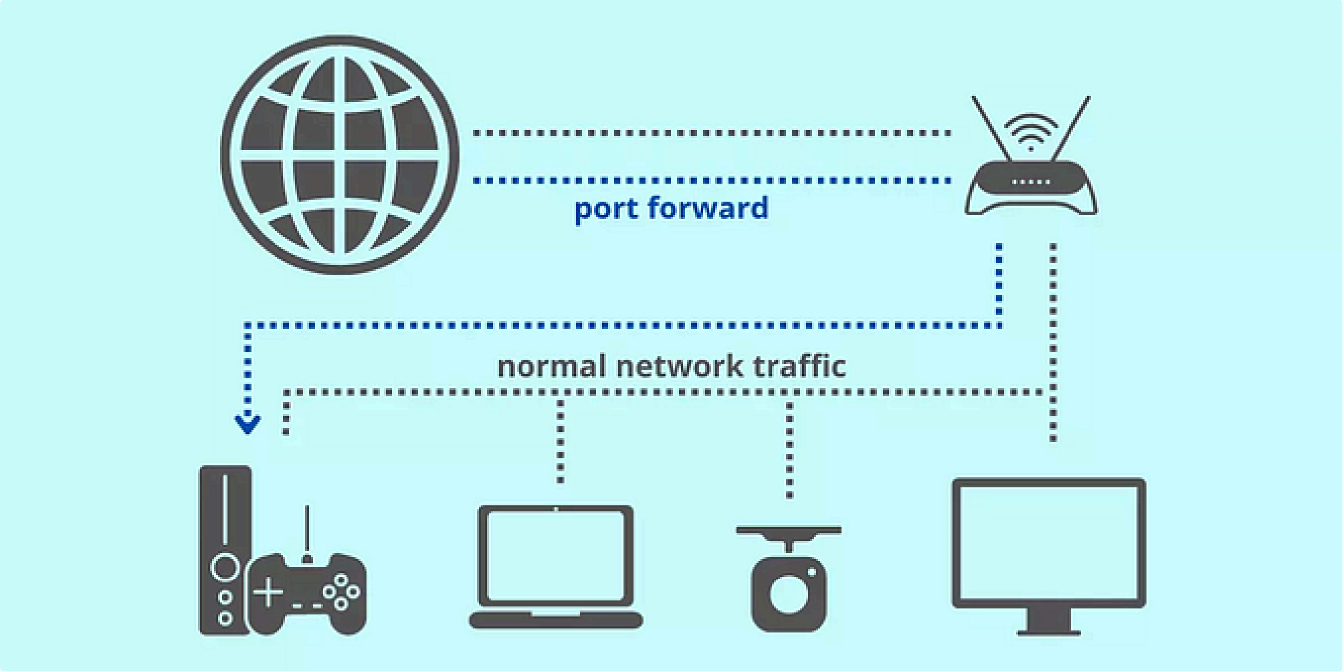
13

Yen

TryHackMe Writeups—Basic Malware RE

Are you ready to dive in the field of Malware Analysis?

3 min read · Nov 11, 2023



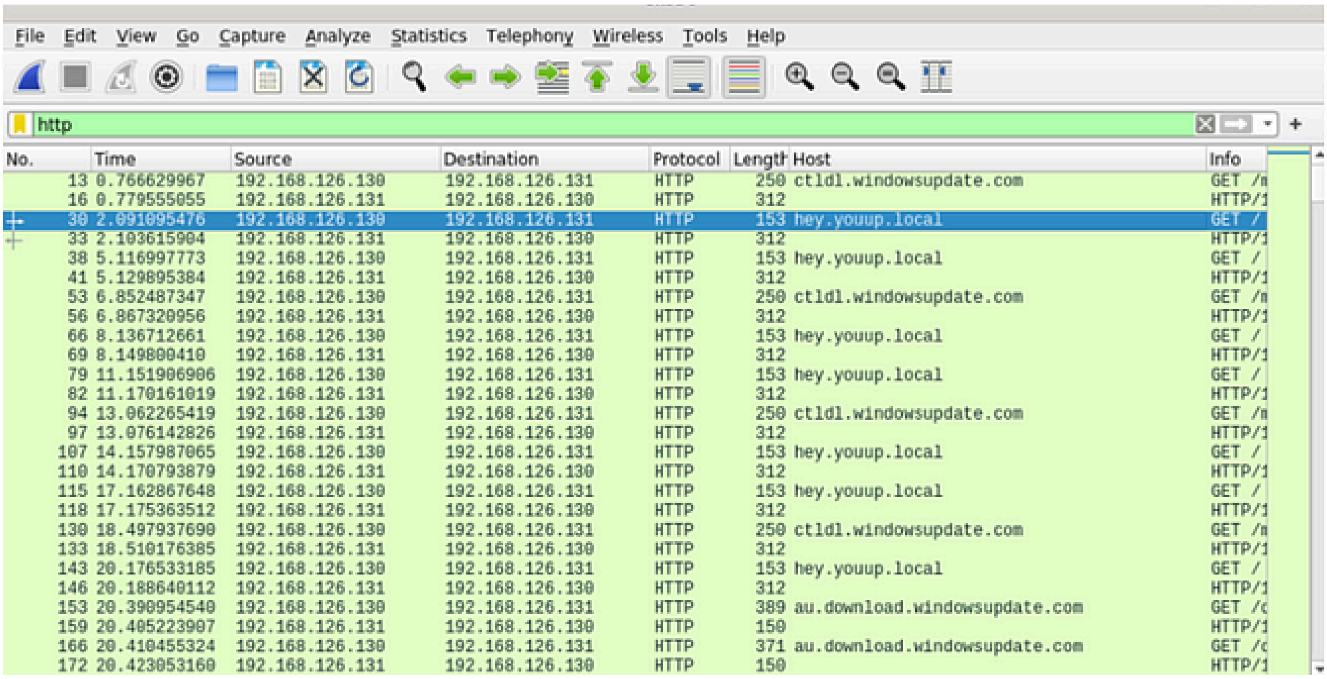
Subhajit Dutta

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



http

No.	Time	Source	Destination	Protocol	Length	Host	Info
13	0.766629967	192.168.126.130	192.168.126.131	HTTP	250	ctldl.windowsupdate.com	GET /n
16	0.779555055	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
30	2.091095476	192.168.126.130	192.168.126.131	HTTP	153	hey.youup.local	GET /
33	2.103615904	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
38	5.116997773	192.168.126.130	192.168.126.131	HTTP	153	hey.youup.local	GET /
41	5.129895384	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
53	6.852487347	192.168.126.130	192.168.126.131	HTTP	250	ctldl.windowsupdate.com	GET /n
56	6.867320956	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
66	8.136712661	192.168.126.130	192.168.126.131	HTTP	153	hey.youup.local	GET /
69	8.149800410	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
79	11.151906906	192.168.126.130	192.168.126.131	HTTP	153	hey.youup.local	GET /
82	11.170161019	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
94	13.062265419	192.168.126.130	192.168.126.131	HTTP	250	ctldl.windowsupdate.com	GET /n
97	13.076142826	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
107	14.157987065	192.168.126.130	192.168.126.131	HTTP	153	hey.youup.local	GET /
110	14.170793879	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
115	17.162867648	192.168.126.130	192.168.126.131	HTTP	153	hey.youup.local	GET /
118	17.175363512	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
130	18.497937690	192.168.126.130	192.168.126.131	HTTP	250	ctldl.windowsupdate.com	GET /n
133	18.510176385	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
143	20.176533185	192.168.126.130	192.168.126.131	HTTP	153	hey.youup.local	GET /
146	20.188640112	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
153	20.390954540	192.168.126.130	192.168.126.131	HTTP	389	au.download.windowsupdate.com	GET /c
159	20.405223907	192.168.126.131	192.168.126.130	HTTP	150		HTTP/1
166	20.410455324	192.168.126.130	192.168.126.131	HTTP	371	au.download.windowsupdate.com	GET /c
172	20.423053160	192.168.126.131	192.168.126.130	HTTP	150		HTTP/1

Hüseyin EKŞİ

Malware Analysis of PMAT-Bonus Unknown malware

I have analyzed the Bonus malware called unknown and would like to share my findings. If you have analyzed this piece of malware please...

3 min read · Jan 21, 2024

13

See more recommendations