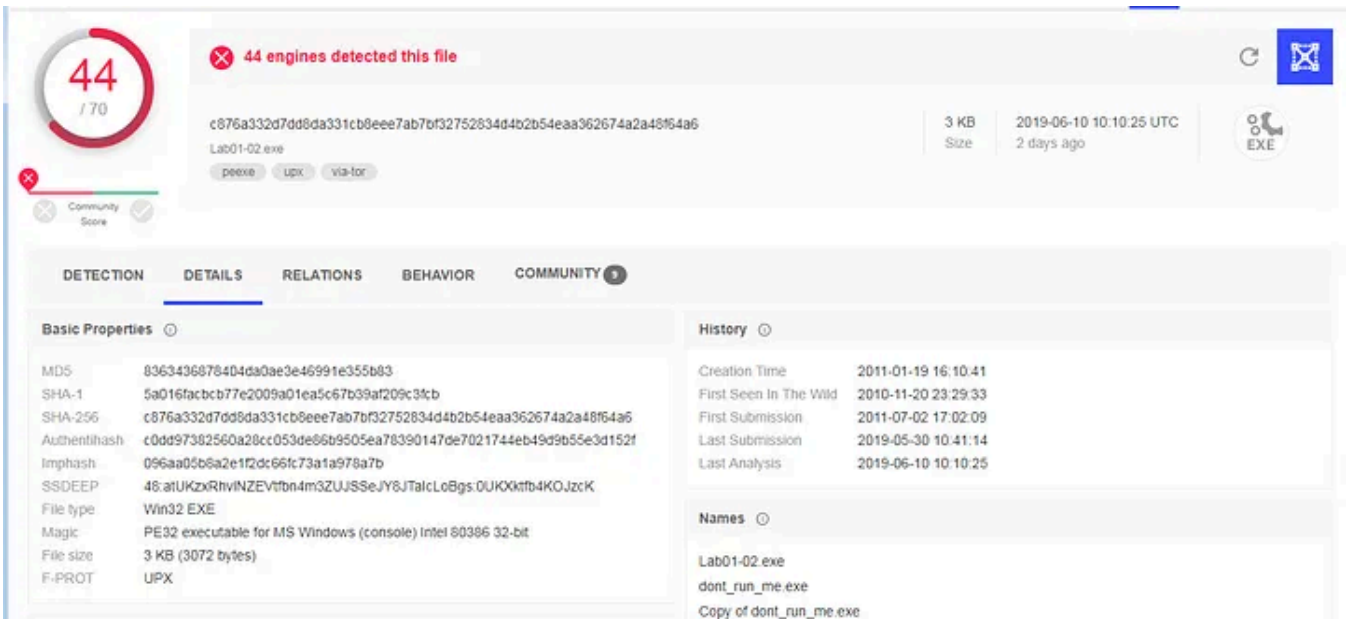
Practical Malware Analysis — Chapter 1 — Lab 1-2 — Solution

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

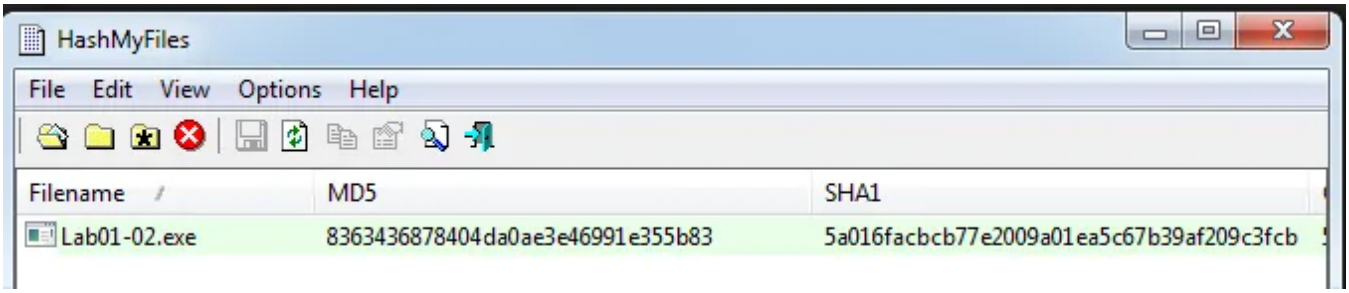
We have recently completed the Lab1–1 questions and found out that it was a



We can see that this file is malicious. This file was created @ 2011–01–19 16:10:41 and fingerprint is as above!

> *MD5 8363436878404da0ae3e46991e355b83*
> *SHA-1 5a016facbcb77e2009a01ea5c67b39af209c3fcb*

Let's use "HashMyFiles" as it can produce no of hashes for a particular file.



We can see that the hashes are same! Now let's try to check the strings!

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

!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
3.04
UPX!
AI3
h(0
L$,
QlI
" z
RV$
u+W
.hP
t=p
sHR
|Pd
 S`
a\`Y
t@E
DmM
;0I
PQ6
(23h
MalService
sHGL345
http://w
warean
ysisbook.co
om#Int6net Explo!r 8FEI
.0<
SystemTimeToFile
GetMo
NaA
Cvg
*Waitab'r
Process
OpenMu$x
ZSB+
ForS
ing
ObjectU4
[Vrtb
CtrlDisp ch
SCM
8_e
Xcpt
mArg
sus
5nm@_
t_fd
```

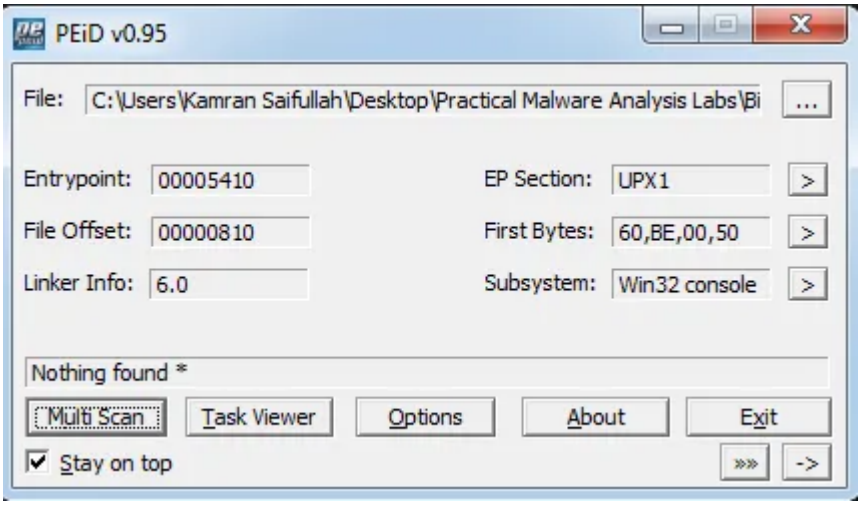
This is the first half and we can clearly see the strings like UPX, UPX0, UPX1, UPX2, UPX3 (UPX is a free and Open-Source Packer for executables) instead of .text, .rdata, .rsrc etc. this probably means that this file is packed. We are able to see URL

(http://ysisbook.co), MalService (Mail Service), Internet Explorer 8FEI (Particular Version) being targeted.

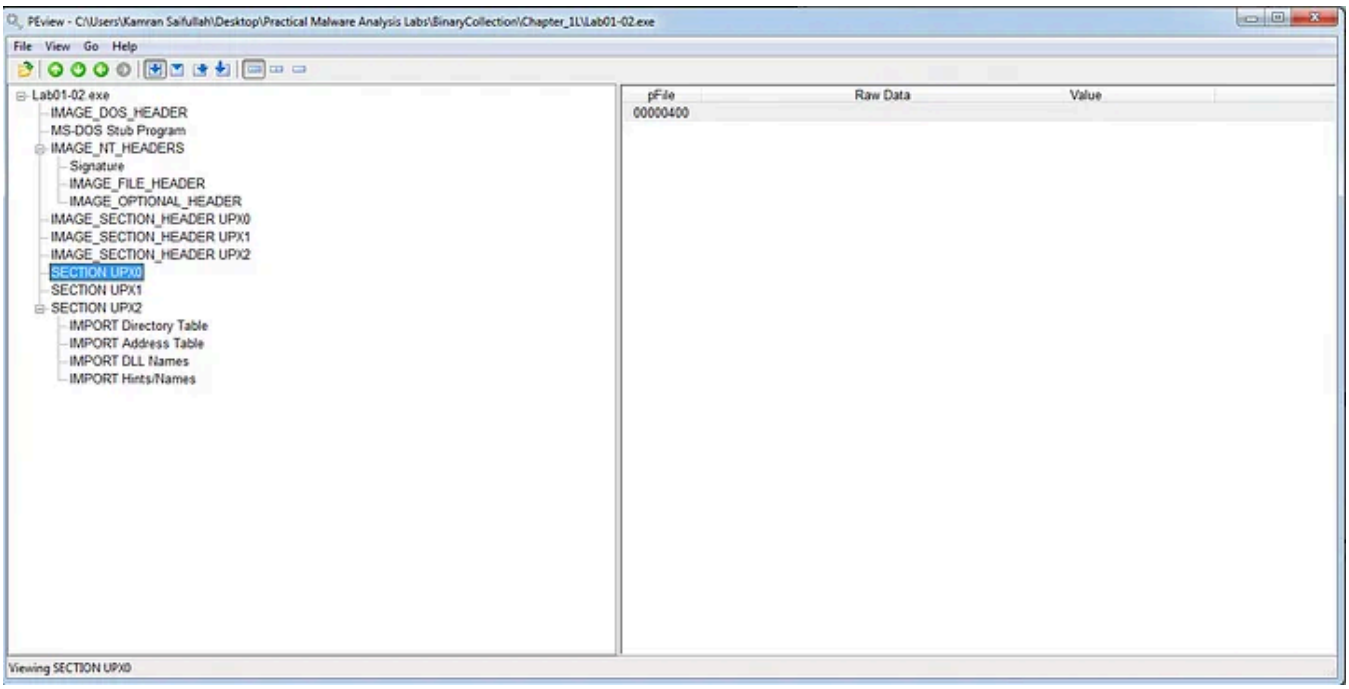
```
i9H
m<e
9,p
vty
dlI37n
olfp
PEL
dW|6
.4t
lB`.rd
@.&
0'0
_~S
u A
GIu
PTj
XPTPSW
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA
```

In the second half we can see the DLL files and some of their functionalities being imported like InternetOpenA, CreateServiceA, Virtual*, [GetProcAddress, LoadLibraryA] these two are most commonly seen in packed executable's.

Let's try running the PEiD on this executable!



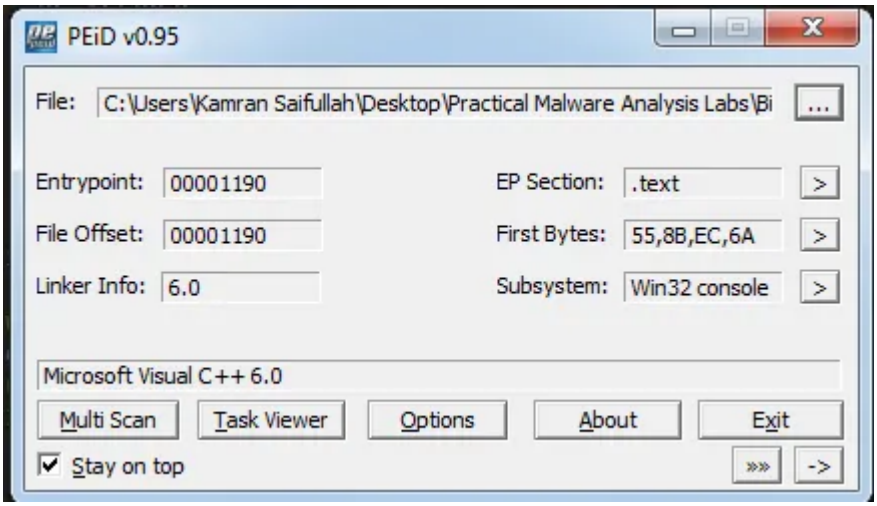
We can see that this executable has been packed using UPX1 as found in EP Section. Now we can analyze the PE Header using PEview and we can clearly seen that the sections have been packed/obfuscated.



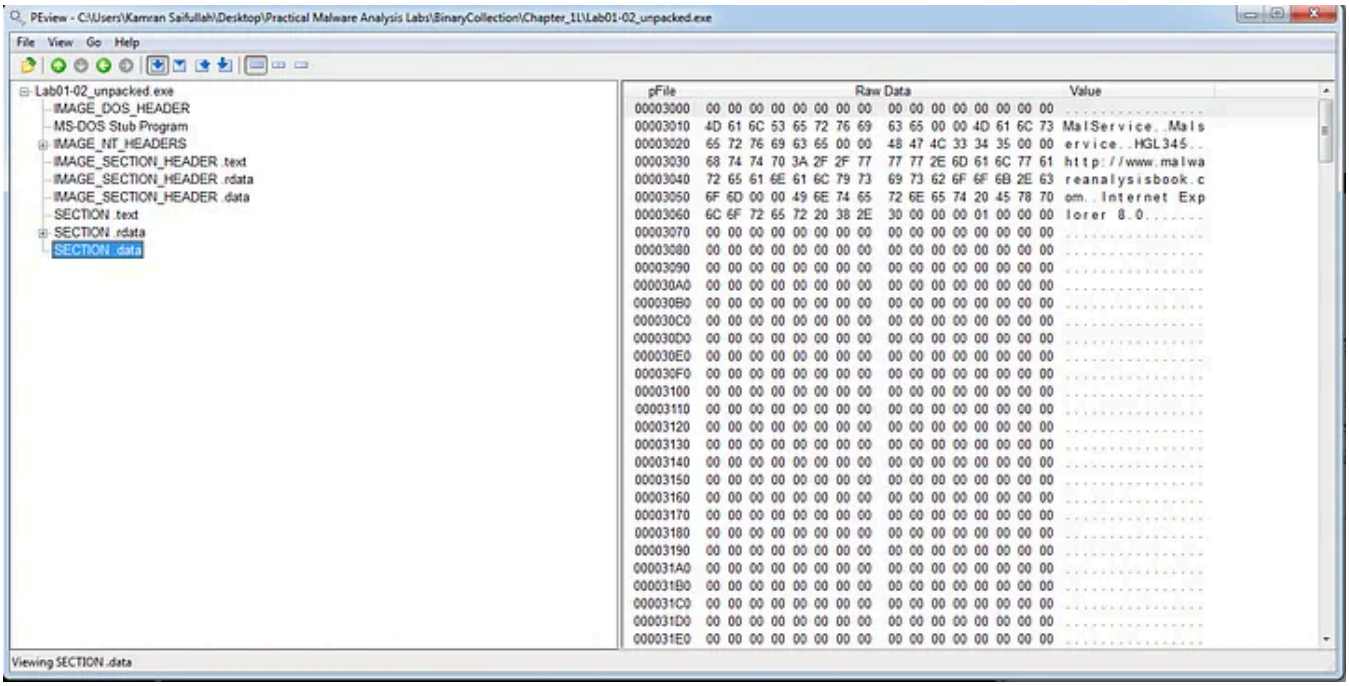
Now we need to unpack this executable. This can be done by using the PE-Explorer plugins and also you can download the UPX tool from github.

```
C:\Users\Kamran Saifullah\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L
λ upx.exe -o Lab01-02_unpacked.exe -d Lab01-02.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95w       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     16384 <-      3072   18.75%    win32/pe     Lab01-02_unpacked.exe

Unpacked 1 file.
```

Let’s run the PEiD on this file now!



We have successfully unpacked the executable. Now we can run the PEview to look for the sections!



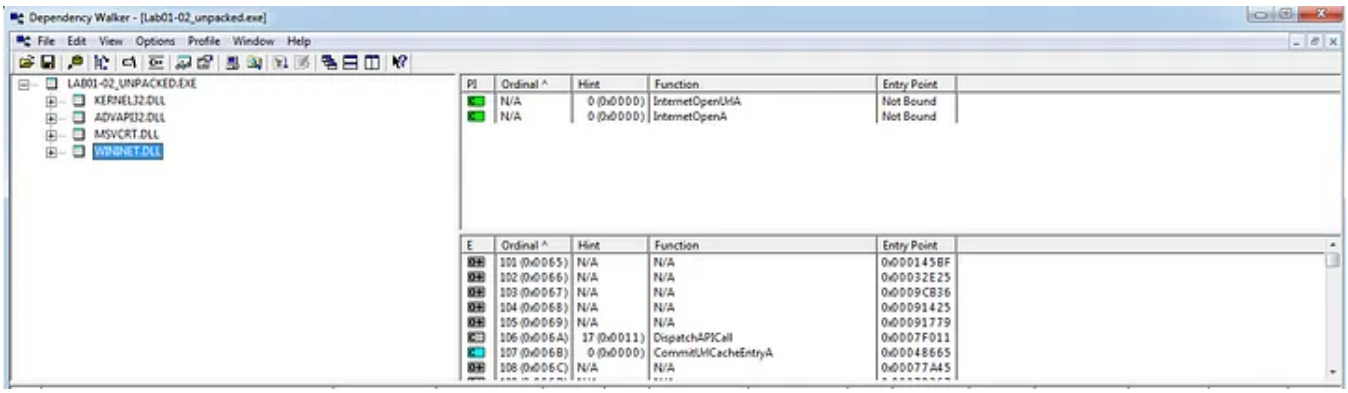
We are able to see the PE Header sections now and the data they contain. At this moment we can run the strings command to check the strings and also DependencyWalker to check the DLL and their corresponding functionalities which are being imported.

On running the strings we are able to see much much more data!

```
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
WININET.dll
SystemTimeToFileTime
GetModuleFileNameA
CreateWaitableTimerA
ExitProcess
OpenMutexA
SetWaitableTimer
WaitForSingleObject
CreateMutexA
CreateThread
CreateServiceA
StartServiceCtrlDispatcherA
OpenSCManagerA
_exit
_XcptFilter
exit
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
InternetOpenUrlA
InternetOpenA
MalService
Malservice
HGL345
http://www.malwareanalysisbook.com
Internet Explorer 8.0

C:\Users\Kamran Saifullah\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L
λ
```

Now we are getting the clearer view of what this executable might do when executed!

On running the DependencyWalker on this executable we can see that it is importing functions from 4 DLLs.



This executable will be connecting to the http://malwareanalysisbook.com and will run it under the name of MalService.

Now that is enough static analysis on this LAB. Let's answer the questions!

Lab 1–2

Analyze the file Lab02–02.exe

Questions

1. **Upload the Lab01–02.exe file to http://www.VirusTotal.com/. Does it match any existing antivirus definitions?**

We have uploaded the file and have found that it matched the existing antivirus definitions.

2. **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?**

We found out that this executable was packed and we were also able to unpack it using the UPX tool.

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

a. InternetOpenA → Initializes an application's use of the WinINet functions we can see what user agent is used to initiate the connection.

b. InternetOpenUrlA → Opens a FTP or HTTP URL

c. CreateMutexA → Create mutex lock to prevent multiple running instances of the malware

d. OpenMutexA → Open a created mutex

e. CreateServiceA → Create a service object to the victim's machine. Often use for persistence.

f. OpenSCManagerA → called before CreateService is invoked to establish a connection to the service control manager

g. StartServiceCtrlDispatcherA → When the service control manager starts a service process, it waits for the process to call the **StartServiceCtrlDispatcher** function. The main thread of a service process should make this call as soon as possible after it starts up (within 30 seconds)

As far as i have understood from the details. This executable is connecting to a website and then binding it as a service MalService for persistence. It's somehow going to be a part of C&C system. Receiving the commands from the web and then executing them on the machine!

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

We can look for the service named MalService via services.msc also we can check for the dnslookups for http://malwareanalysisbook.com/ via a specific Internet Explorer string which will be passed via the browser user-agent FIELD. Moreover we can create a firewall rule to block such traffic.

Security

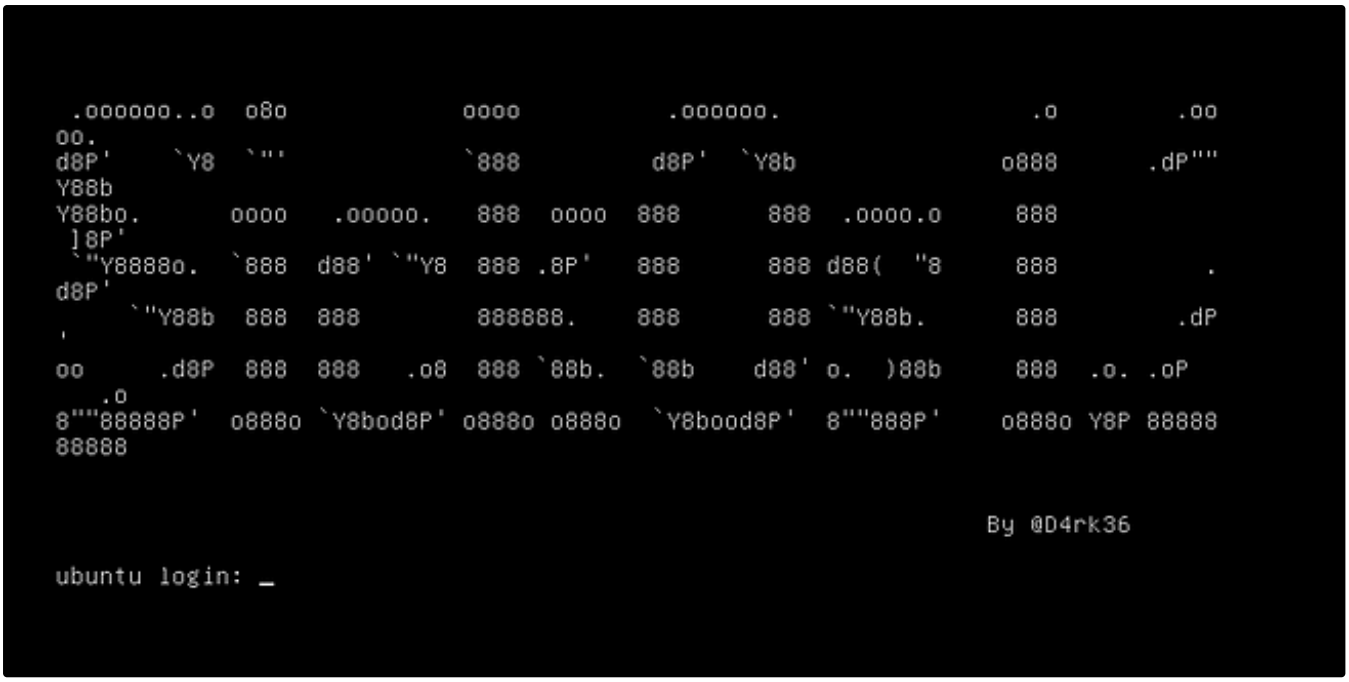
Follow

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



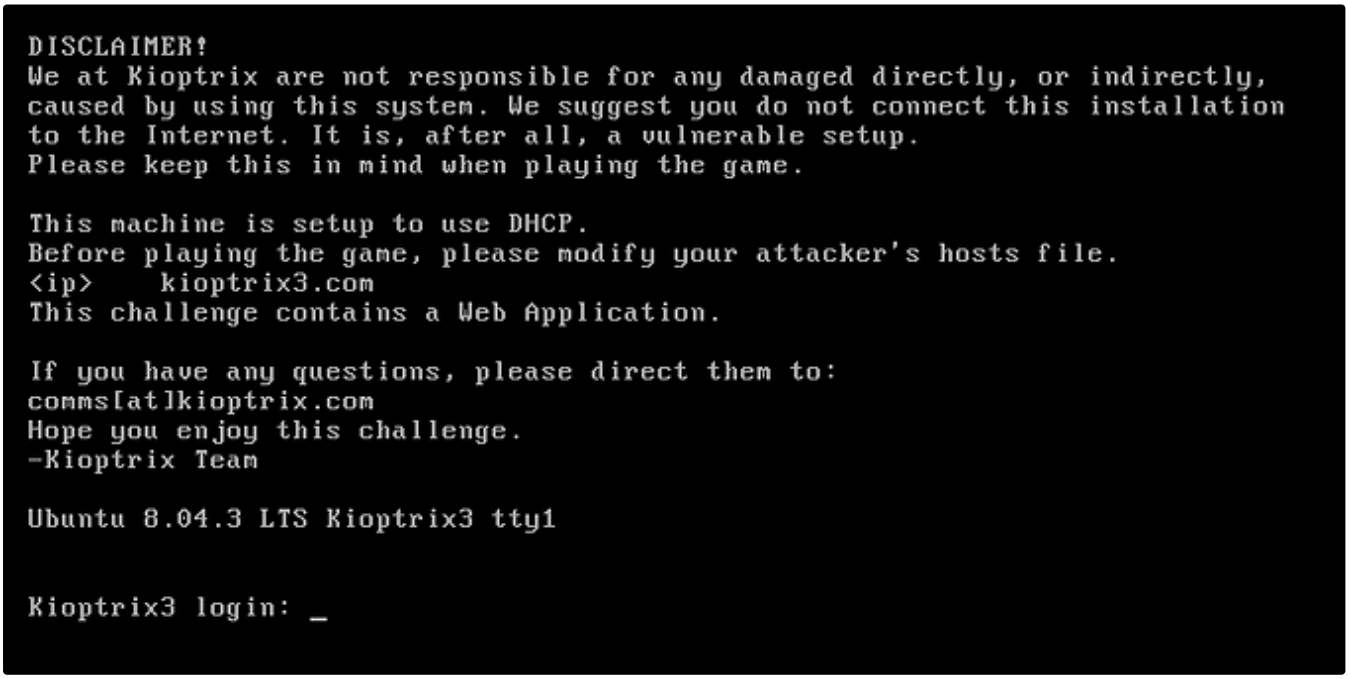
Kamran Saifullah

SickOS 1.2 WalkThrough

Hi,

5 min read · Apr 14, 2018

10



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.

hsctf-chicke...

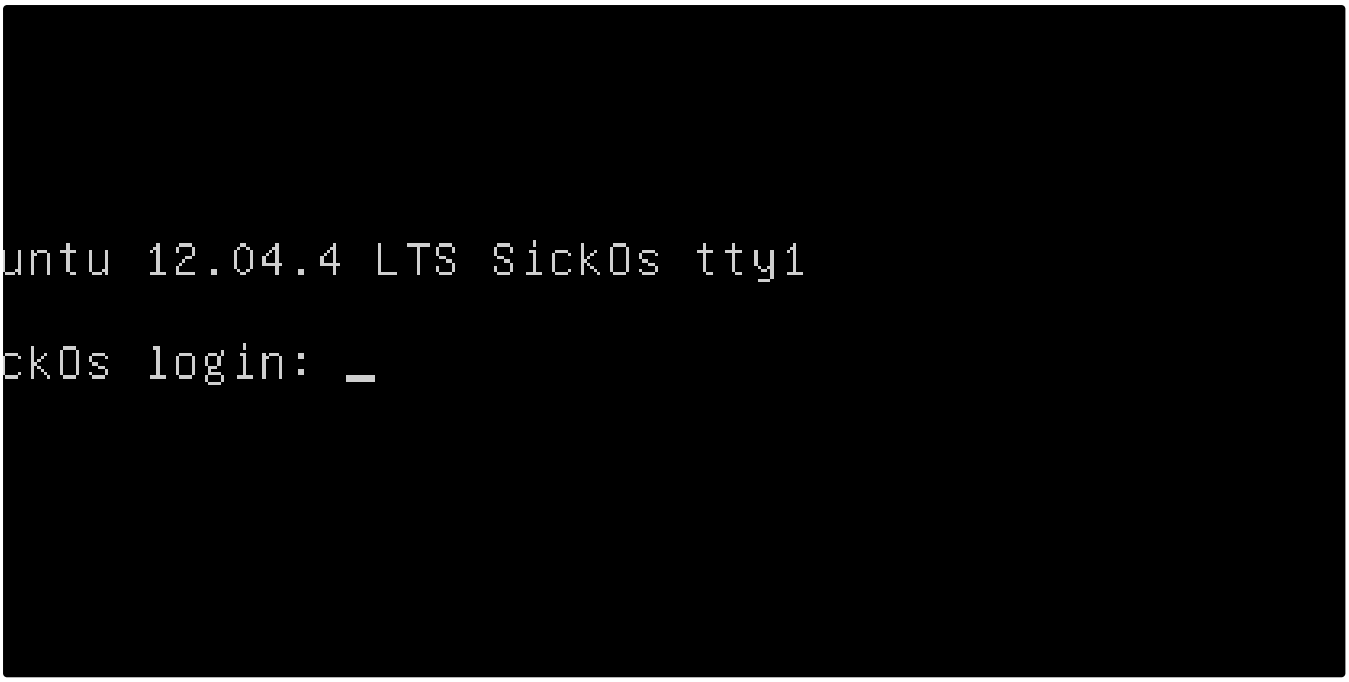
Kamran Saifullah

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



Kamran Saifullah

SickOS 1.1 Walkthrough

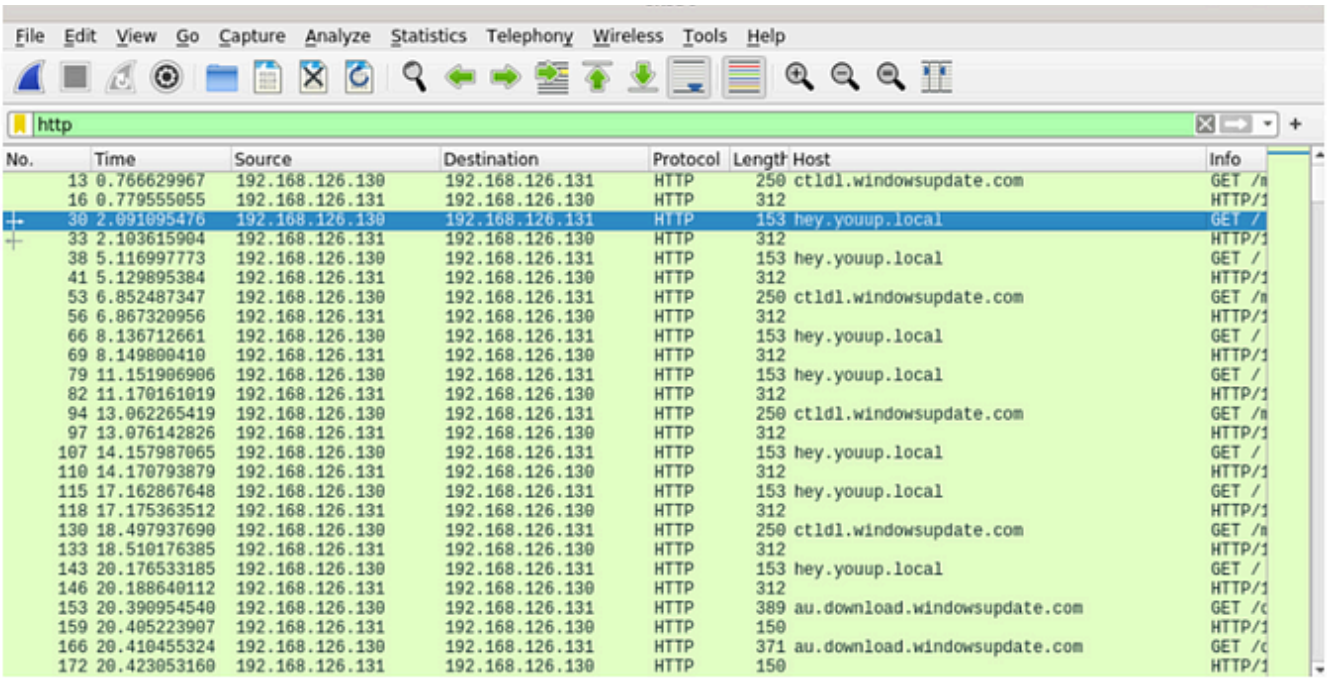
Hi,

5 min read · Apr 11, 2018

9

See all from Kamran Saifullah

Recommended from Medium



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

Abdelwahab Shandy

CyberDefenders :Qradar101 Blue Team Challenge

Category : Threat Hunting

11 min read · Nov 23, 2023

4

Lists

Staff Picks

630 stories · 920 saves

Stories to Help You Level-Up at Work

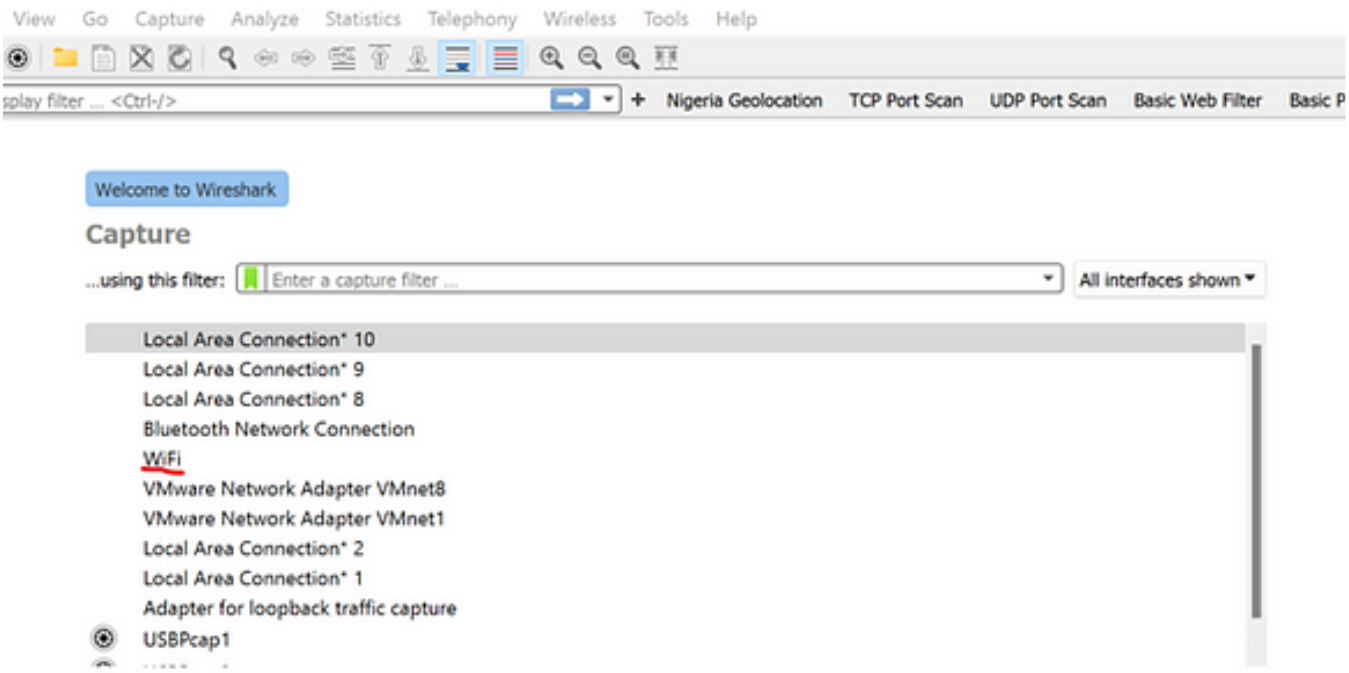
19 stories · 581 saves

Self-Improvement 101

20 stories · 1675 saves

Productivity 101

20 stories · 1543 saves



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

Rewa Aslekar

Malware Analysis

A Beginner's guide to Malware Analysis

13 min read · Oct 31, 2023

16

Yen

TryHackMe Writeups—Basic Malware RE

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

3 min read · Nov 11, 2023

Worldsleaks

OpenWire—

CyberDefenders CTF

7 min read · Jan 25, 2024

13

See more recommendations