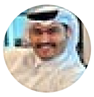
Practical Malware Analysis — Chapter 3 — Lab03 -03 — Solution



Kamran Saifullah · Follow

3 min read · Aug 29, 2019

Listen Share

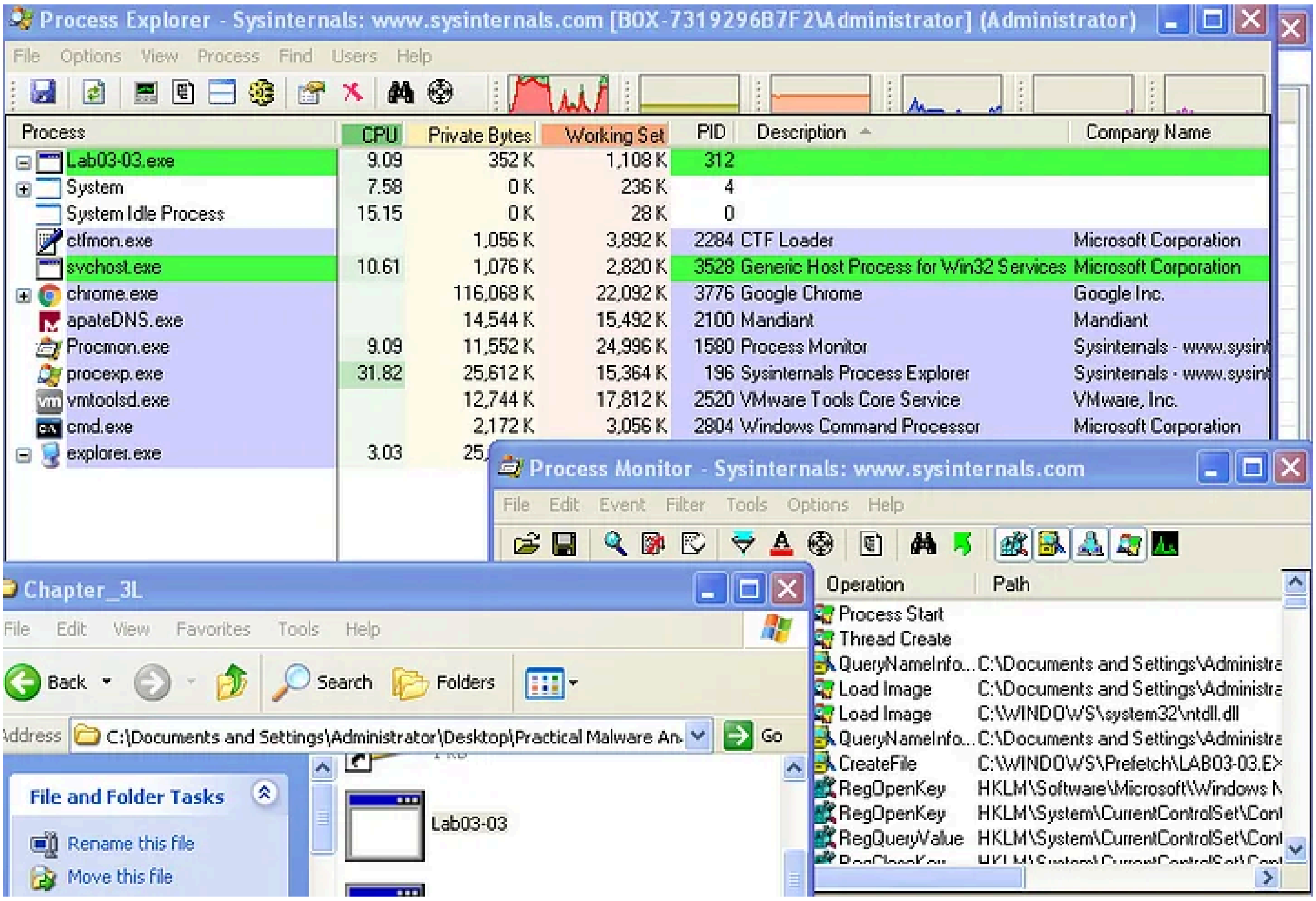
Now we are going to analyze the Lab03–03.exe. Starting with the strings for basic static analysis.

> *!This program cannot be run in DOS mode.*
>
> *Rich*
>
> *.text*
>
> *`.rdata*
>
> *@.data*
>
> *.rsrc*
>
> *Microsoft Visual C++ Runtime Library*
>
> *Runtime Error!*
>
> *Program:*
>
> *…*
>
> *<program name unknown>*
>
> *GetLastActivePopup*
>
> *GetActiveWindow*
>
> *MessageBoxA*
>
> ***user32.dll***
>
> *=9@*
>
> *A9@*
>
> *CloseHandle*
>
> *VirtualFree*
>
> *ReadFile*

> *VirtualAlloc*
>
> *GetFileSize*
>
> ***CreateFileA***
>
> *ResumeThread*
>
> *SetThreadContext*
>
> *WriteProcessMemory*
>
> *VirtualAllocEx*
>
> *GetProcAddress*
>
> *GetModuleHandleA*
>
> *ReadProcessMemory*
>
> *GetThreadContext*
>
> ***CreateProcessA***
>
> *FreeResource*
>
> *SizeofResource*
>
> *LockResource*
>
> *LoadResource*
>
> *FindResourceA*
>
> *GetSystemDirectoryA*
>
> *Sleep*
>
> ***KERNEL32.dll***
>
> *GetCommandLineA*
>
> *GetVersion*
>
> *ExitProcess*
>
> *TerminateProcess*
>
> *GetCurrentProcess*
>
> *UnhandledExceptionFilter*
>
> *GetModuleFileNameA*
>
> *FreeEnvironmentStringsA*
>
> *FreeEnvironmentStringsW*
>
> *WideCharToMultiByte*
>
> *GetEnvironmentStrings*
>
> *GetEnvironmentStringsW*
>
> *SetHandleCount*
>
> *GetStdHandle*

> *HeapCreate*
>
> *HeapFree*
>
> *RtlUnwind*
>
> *WriteFile*
>
> *HeapAlloc*
>
> *GetCPInfo*
>
> *GetACP*
>
> *GetOEMCP*
>
> *HeapReAlloc*
>
> ***LoadLibraryA***
>
> *MultiByteToWideChar*
>
> *LCMapStringA*
>
> *LCMapStringW*
>
> *GetStringTypeA*
>
> *GetStringTypeW*
>
> *h-@*
>
> *\svchost.exe*
>
> *NtUnmapViewOfSection*
>
> ***ntdll.dll***
>
> *UNICODE*
>
> *LOCALIZATION*

This seems to be a packed executable. Now we will directly move onto performing the Basic Dynamic Analysis.

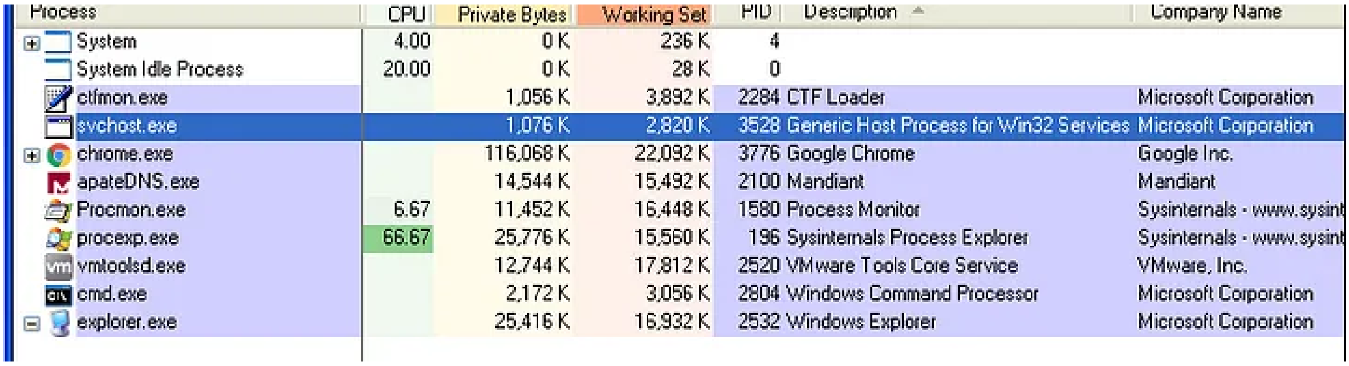

Process Explorer - Sysinternals: www.sysinternals.com [BOX-7319296B7F2\Administrator] (Administrator)
File Options View Process Find Users Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Chapter_3L
File Edit View Favorites Tools Help
Back
Search
Folders
Address
Go
File and Folder Tasks
Rename this file
Move this file
Lab03-03

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Lab03-03.exe	9.09	352 K	1,108 K	312		
System	7.58	0 K	236 K	4		
System Idle Process	15.15	0 K	28 K	0		
ctfmon.exe		1,056 K	3,892 K	2284	CTF Loader	Microsoft Corporation
svchost.exe	10.61	1,076 K	2,820 K	3528	Generic Host Process for Win32 Services	Microsoft Corporation
chrome.exe		116,068 K	22,092 K	3776	Google Chrome	Google Inc.
apateDNS.exe		14,544 K	15,492 K	2100	Mandiant	Mandiant
Procmon.exe	9.09	11,552 K	24,996 K	1580	Process Monitor	Sysinternals - www.sysint
procexp.exe	31.82	25,612 K	15,364 K	196	Sysinternals Process Explorer	Sysinternals - www.sysint
vmtoolsd.exe		12,744 K	17,812 K	2520	VMware Tools Core Service	VMware, Inc.
cmd.exe		2,172 K	3,056 K	2804	Windows Command Processor	Microsoft Corporation
explorer.exe	3.03	25,				

C:\Documents and Settings\Administrator\Desktop\Practical Malware An

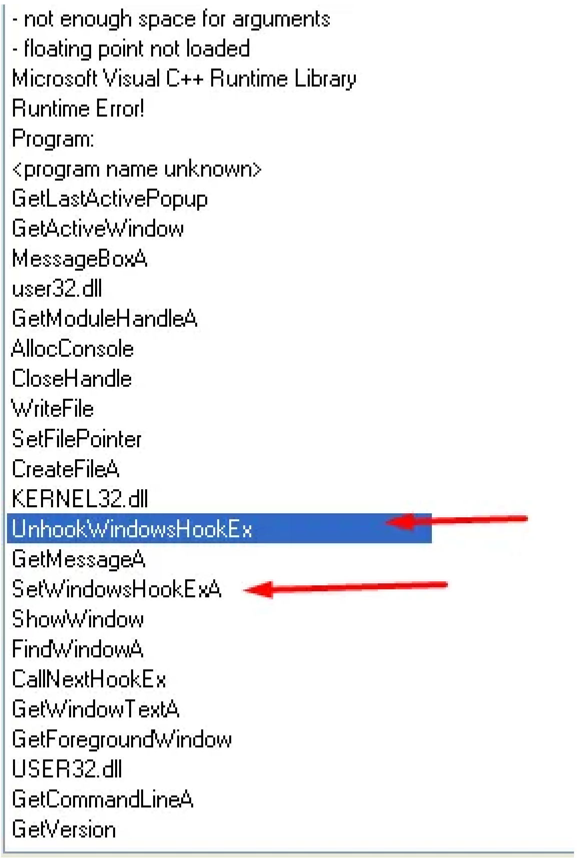
Operation	Path
Process Start	
Thread Create	
QueryNameInfo...	C:\Documents and Settings\Administra
Load Image	C:\Documents and Settings\Administra
Load Image	C:\WINDOWS\system32\ntdll.dll
QueryNameInfo...	C:\Documents and Settings\Administra
CreateFile	C:\WINDOWS\Prefetch\LAB03-03.EX
RegOpenKey	HKLM\Software\Microsoft\Windows N
RegOpenKey	HKLM\System\CurrentControlSet\Cont
RegQueryValue	HKLM\System\CurrentControlSet\Cont

On running the malware we can see it in the explorer. But within 2 seconds the actual executable is removed.



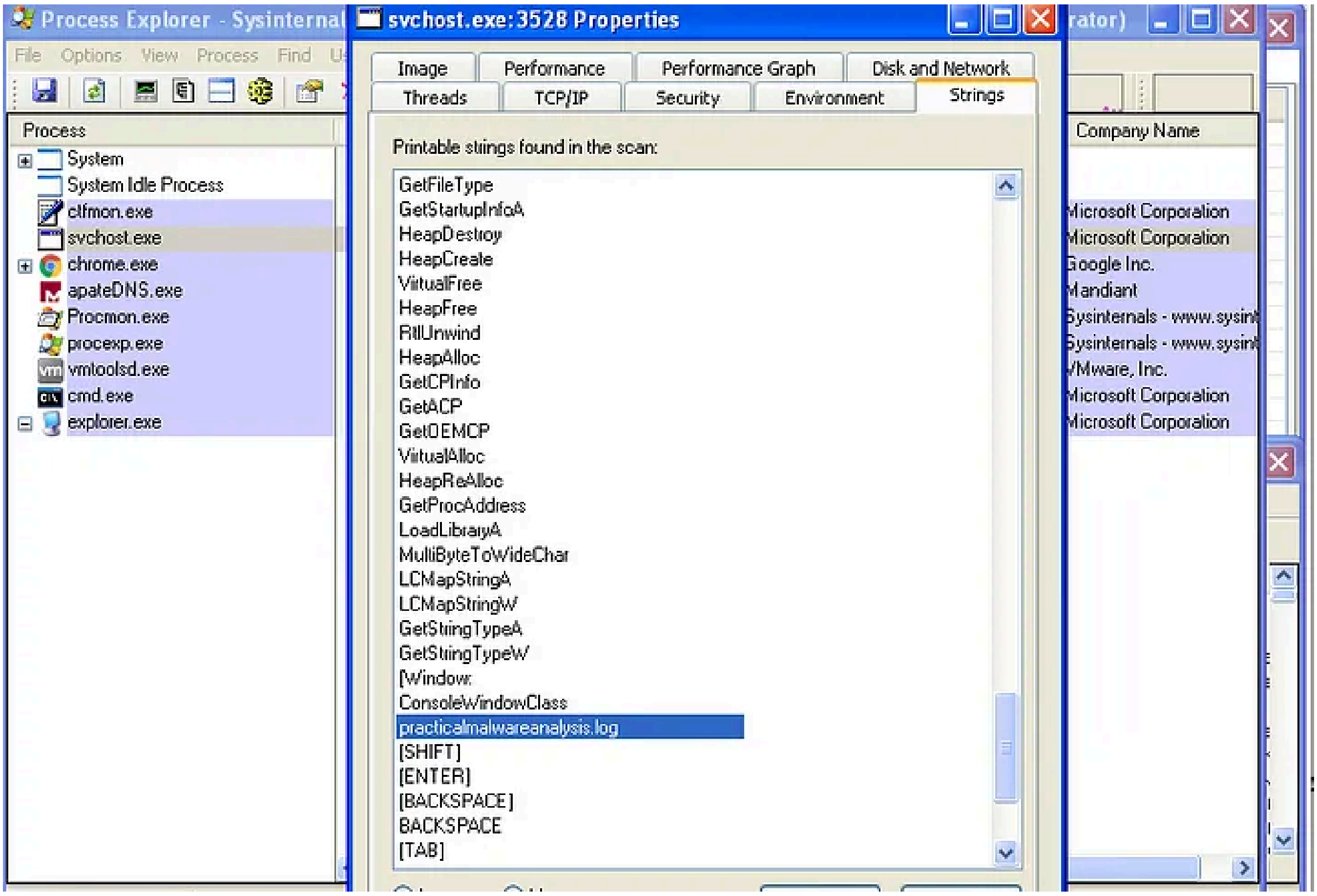
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System	4.00	0 K	236 K	4		
System Idle Process	20.00	0 K	28 K	0		
ctfmon.exe		1,056 K	3,892 K	2284	CTF Loader	Microsoft Corporation
svchost.exe		1,076 K	2,820 K	3528	Generic Host Process for Win32 Services	Microsoft Corporation
chrome.exe		116,068 K	22,092 K	3776	Google Chrome	Google Inc.
apateDNS.exe		14,544 K	15,492 K	2100	Mandiant	Mandiant
Procmon.exe	6.67	11,452 K	16,448 K	1580	Process Monitor	Sysinternals - www.sysint
procexp.exe	66.67	25,776 K	15,560 K	196	Sysinternals Process Explorer	Sysinternals - www.sysint
vmtoolsd.exe		12,744 K	17,812 K	2520	VMware Tools Core Service	VMware, Inc.
cmd.exe		2,172 K	3,056 K	2804	Windows Command Processor	Microsoft Corporation
explorer.exe		25,416 K	16,932 K	2532	Windows Explorer	Microsoft Corporation

The svchost.exe is left abandoned and orphan. On checking the strings in the memory of svchost.exe we find this executable to be a keylogger.



```
- not enough space for arguments
- floating point not loaded
Microsoft Visual C++ Runtime Library
Runtime Error!
Program:
<program name unknown>
GetLastActivePopup
GetActiveWindow
MessageBoxA
user32.dll
GetModuleHandleA
AllocConsole
CloseHandle
WriteFile
SetFilePointer
CreateFileA
KERNEL32.dll
UnhookWindowsHookEx
GetMessageA
SetWindowsHookExA
ShowWindow
FindWindowA
CallNextHookEx
GetWindowTextA
GetForegroundWindow
USER32.dll
GetCommandLineA
GetVersion
```

Also we can see that log file is being created. Which for sure will be keeping track of our keystrokes.

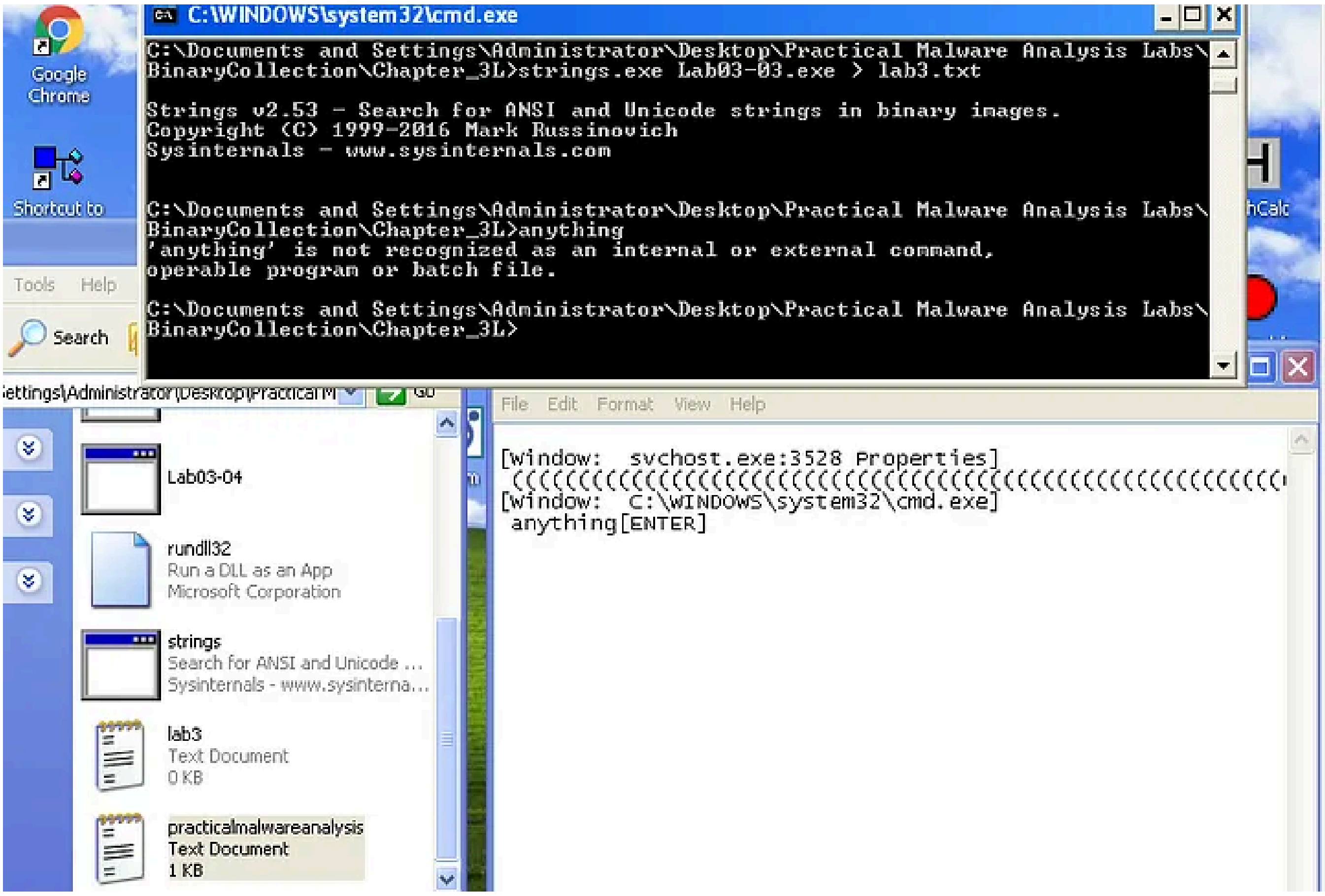


Process	Company Name
System	
System Idle Process	
clfmon.exe	Microsoft Corporation
svchost.exe	Microsoft Corporation
chrome.exe	Google Inc.
apateDNS.exe	Mandiant
Procmon.exe	Sysinternals - www.sysint
procexp.exe	Sysinternals - www.sysint
vmtoolsd.exe	VMware, Inc.
cmd.exe	Microsoft Corporation
explorer.exe	Microsoft Corporation

Printable strings found in the scan:

```
GetFileType
GetStartupInfoA
HeapDestroy
HeapCreate
VirtualFree
HeapFree
RtlUnwind
HeapAlloc
GetCPInfo
GetACP
GetOEMCP
VirtualAlloc
HeapReAlloc
GetProcAddress
LoadLibraryA
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
[Window:
ConsoleWindowClass
practicalmalwareanalysis.log
[SHIFT]
[ENTER]
[BACKSPACE]
BACKSPACE
[TAB]
```

Here we have it.



```
C:\Documents and Settings\Administrator\Desktop\Practical Malware Analysis Labs\
BinaryCollection\Chapter_3L>strings.exe Lab03-03.exe > lab3.txt

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


C:\Documents and Settings\Administrator\Desktop\Practical Malware Analysis Labs\
BinaryCollection\Chapter_3L>anything
'anything' is not recognized as an internal or external command,
operable program or batch file.

C:\Documents and Settings\Administrator\Desktop\Practical Malware Analysis Labs\
BinaryCollection\Chapter_3L>
```

```
[Window:  svchost.exe:3528 Properties]
 ((((((((((((((((((((((((((((((((((((((((((((((((((((((
[Window:  C:\WINDOWS\system32\cmd.exe]
 anything[ENTER]
```

Now it’s time to answer the questions.

Lab 3–3

Execute the malware found in the file Lab03–03.exe while monitoring it using basic dynamic analysis tools in a safe environment.

Questions

1. What do you notice when monitoring this malware with Process Explorer?

We notice that when the malware is run. The actual process is shown which then creates the child process and then removes itself leaving an orphan process.

2. Can you identify any live memory modifications?

We can identify the live memory modifications by looking onto the memory strings as they reveal the strings after the malware is run in the memory. In those strings we can actually see the HOOK and log file from which we concluded that this executable is a Keylogger.

3. What are the malware’s host-based indicators?

The host-based indicators for this malware is the file “practicalmalwareanalysis.log” presence on the system.

4. What is the purpose of this program?

The purpose of this program is to log all of the keystrokes from the keyboard and then save them into the log file.

Security

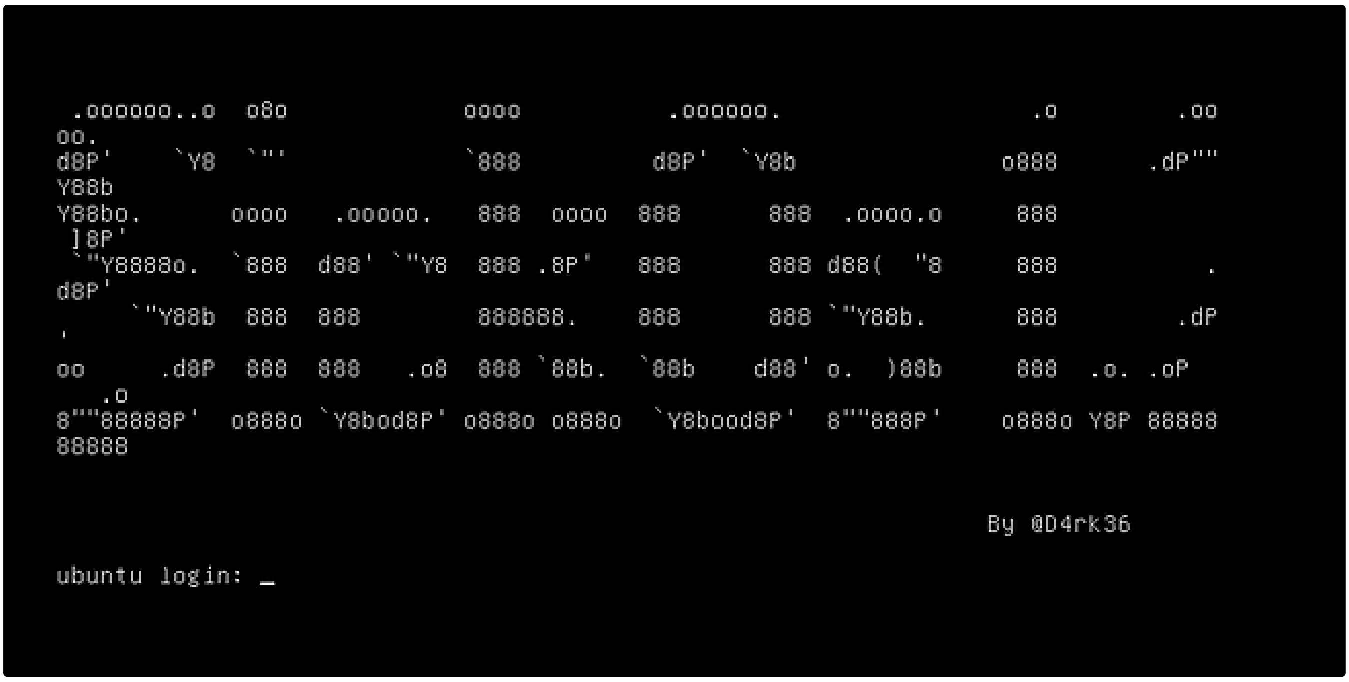
Follow

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



```
  .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: _
```

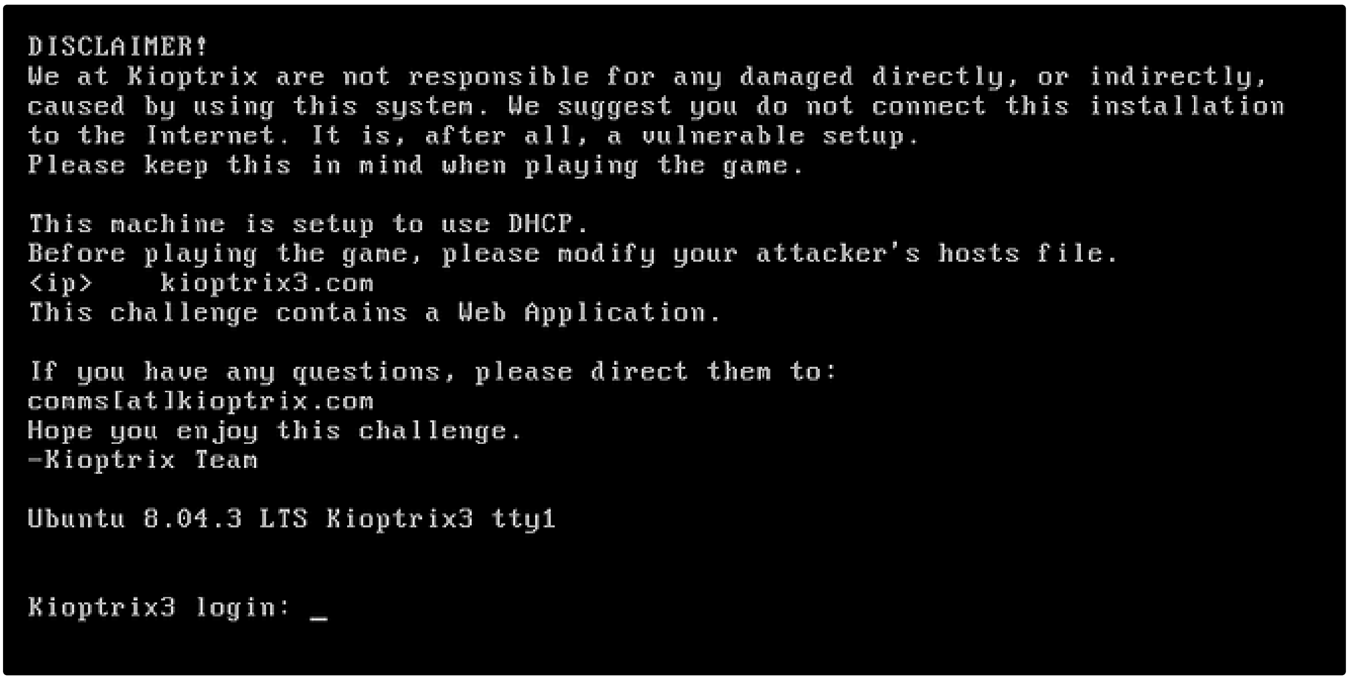
Kamran Saifullah

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.

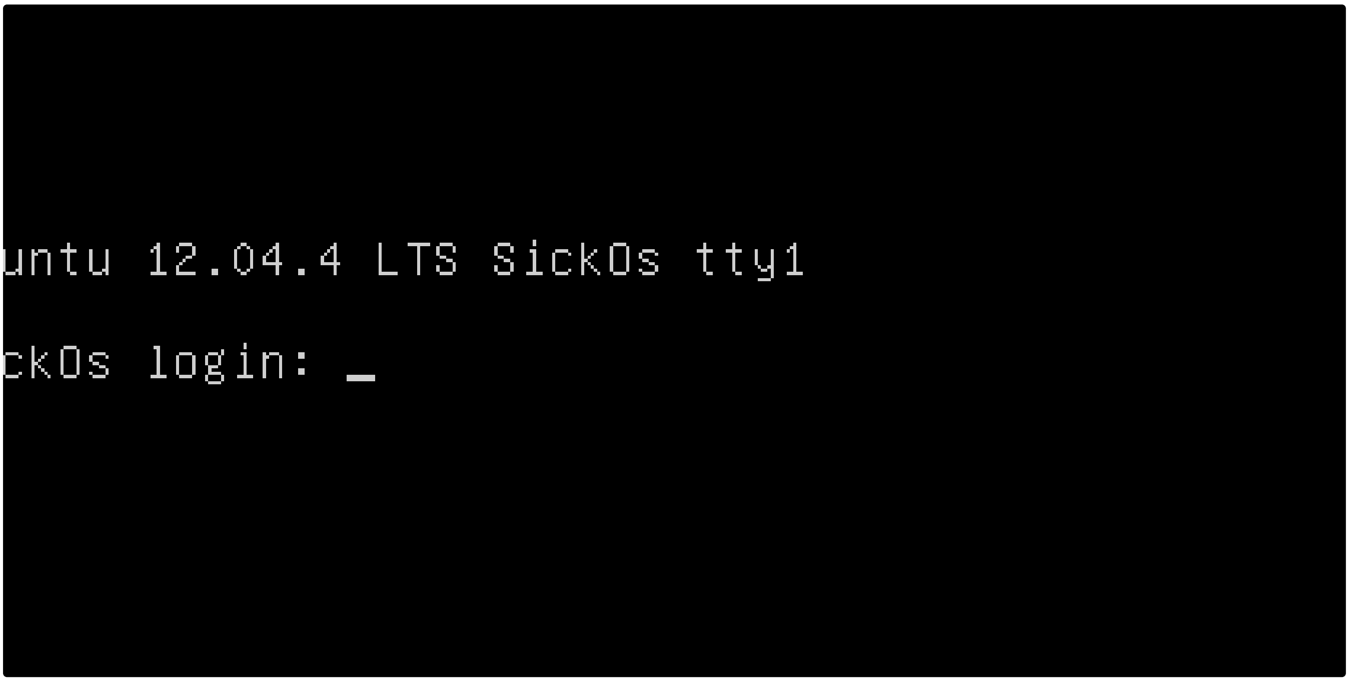
Kamran Saifullah

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

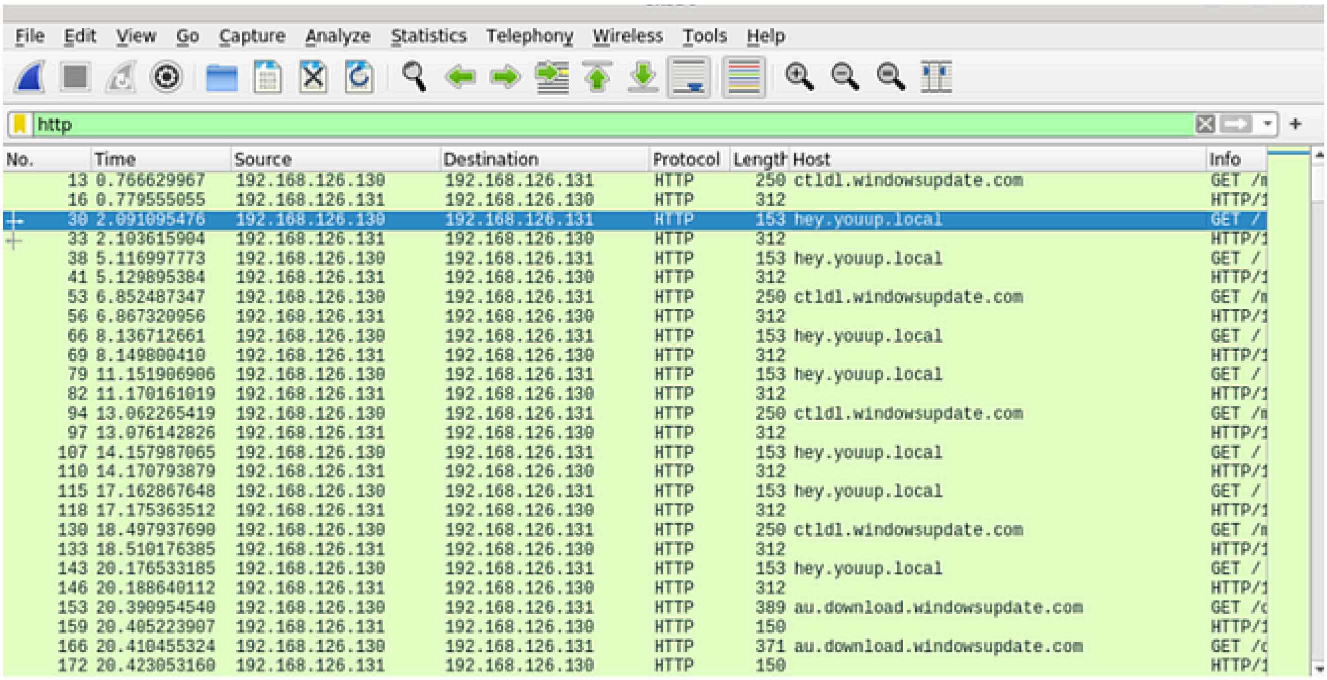
Hi,

5 min read · Apr 11, 2018

9

See all from Kamran Saifullah

Recommended from Medium



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

Abdelwahab Shandy

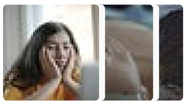
CyberDefenders :Qradar101 Blue Team Challenge

Category : Threat Hunting

11 min read · Nov 23, 2023

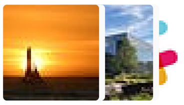
4

Lists



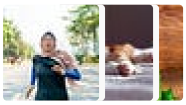
Staff Picks

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

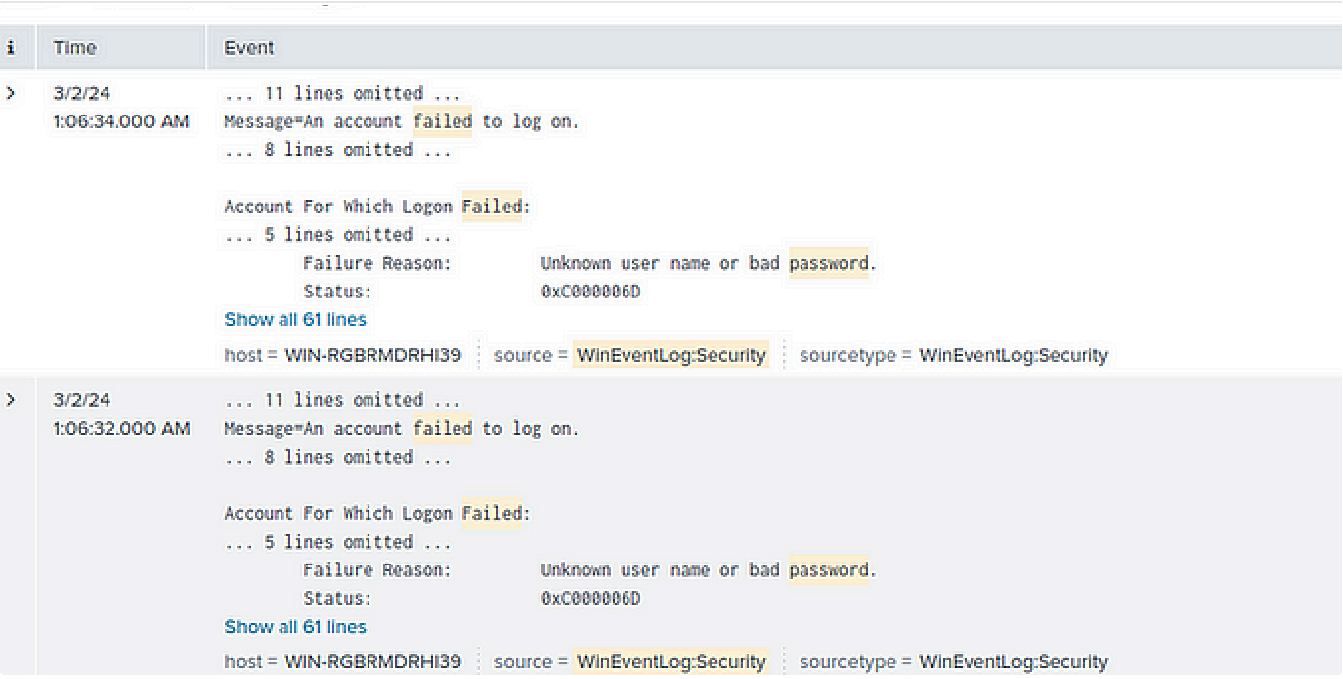
```
 25 11:53:38 2023 as: nmap -sCVS -vvv -oA nmap/exfiltrated 192.168.216.163
63
l 61 (0.27s latency).
 for 111s
eset)
  VERSION
1 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)

5:28:d3:63:b4:48:bb:cf (RSA)
AAABgQDH6PH1/ST7TUJ4Mp/l4c7G+TM07YbX7YIsnHzq1TRpvtiBhdNQufkL15NW9+za+h6ZraqoZ0ewwkH+0La4361DQ+2H/Nh4Cn1J0rRbpLJKg4hChjgCHd5KiLC0KHhXPs/FA3mm
D4Mu17wB5w6yvXyj+lleKjQ6Hnje7KorW5q4U6ijd3LmvHE34UHg/qUbCUbiwY06N2MjBNQiZqWN8z48eTzGsuh6u1SfGIDnCCq3sWm37Y5LIUvqAFy1EJZVsC/UyrJOPBE+YIODNbN2Q
3SNqUq2enfPwQt39nigtUercckdyUD0oRKqVnhZCjEYfX3qOnlAqejr3LpmBnA31pp8lrKNAmQEjdSO8Jsk04OR2JBxcfVNfs=
:f0:36:ac:19:d8:0e:f3 (ECDSA)
LXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBI0EdIHR7NORxMM0G7C8zxbLgwB3ump+nb2D3Pe3tXqp/6jNJ/GbUZe4Ab44njMKHJbm/PzrtYzojMjGDu8lQCg=
:f4:80:8d:33:ce:9b:3a (ED25519)
AAAAIDCc0saExmeDXtqm5FS+D5RmDke8aJEvFq1DJIr0KZML
1 Apache httpd 2.4.41 ((Ubuntu))
tries
l/ /panel/ /tmp/

5: 09BDDB30D6AE11E854BFF82ED638542B
ect to http://exfiltrated.offsec/
1 (Ubuntu)

ST OPTIONS
/o:linux:linux_kernel

share/nmap
e report any incorrect results at https://nmap.org/submit/ .
 2023 -- 1 IP address (1 host up) scanned in 118.16 seconds
```

Ardian Danny

[OSCP Practice Series 1] Proving Grounds — Exfiltrated

Machine Type: Linux

3 min read · Dec 26, 2023



i	Time	Event
>	3/2/24 1:06:34.000 AM	... 11 lines omitted ... Message=An account failed to log on. ... 8 lines omitted ... Account For Which Logon Failed: ... 5 lines omitted ... Failure Reason: Unknown user name or bad password. Status: 0xC000006D Show all 61 lines host = WIN-RGBRMDRHI39 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	3/2/24 1:06:32.000 AM	... 11 lines omitted ... Message=An account failed to log on. ... 8 lines omitted ... Account For Which Logon Failed: ... 5 lines omitted ... Failure Reason: Unknown user name or bad password. Status: 0xC000006D Show all 61 lines host = WIN-RGBRMDRHI39 source = WinEventLog:Security sourcetype = WinEventLog:Security

Sulaiman Syed

Threat Detection using Splunk

This lab covers how to ingest data into Splunk and monitor the events of an Active Directory domain to discover potential threats. It will...

8 min read · Mar 4, 2024

26

Rewa Aslekar

Malware Analysis

A Beginner’s guide to Malware Analysis

13 min read · Oct 31, 2023

16

Zaid Khaishagi

GHIDRA TUTORIAL: CTF CHALLENGE

This is the final article in the Ghidra Tutorial series. In this tutorial, we will make use of Ghidra to solve an actual CTF challenge. We...

8 min read · Jan 2, 2024

14

See more recommendations