

Open in app ↗

Sign up

Sign in



Search



LABS

The purpose of the labs is to give you an opportunity to practice the skills taught in the chapter. In order to simulate realistic malware analysis you will be given little or no information about the program you are analyzing. Like all of the labs throughout this book, the basic static analysis lab files have been given generic names to simulate unknown malware, which typically use meaningless or misleading names.

Each of the labs consists of a malicious file, a few questions, short answers to the questions, and a detailed analysis of the malware. The solutions to the labs are included in Appendix C.

The labs include two sections of answers. The first section consists of short answers, which should be used if you did the lab yourself and just want to check your work. The second section includes detailed explanations for you to follow along with our solution and learn how we found the answers to the questions posed in each lab.

Practical Malware Analysis — Book

Practical Malware Analysis — Chapter 1 — Labs 1-1 — Solution

Kamran Saifullah · [Follow](#)

4 min read · Aug 29, 2019



Listen



Share

As we are done with the Chapter-1. It's time to work on the labs to get most out of our learning. So let's begin.

Note: I have copied the Labs Details (text) from the book as it is.

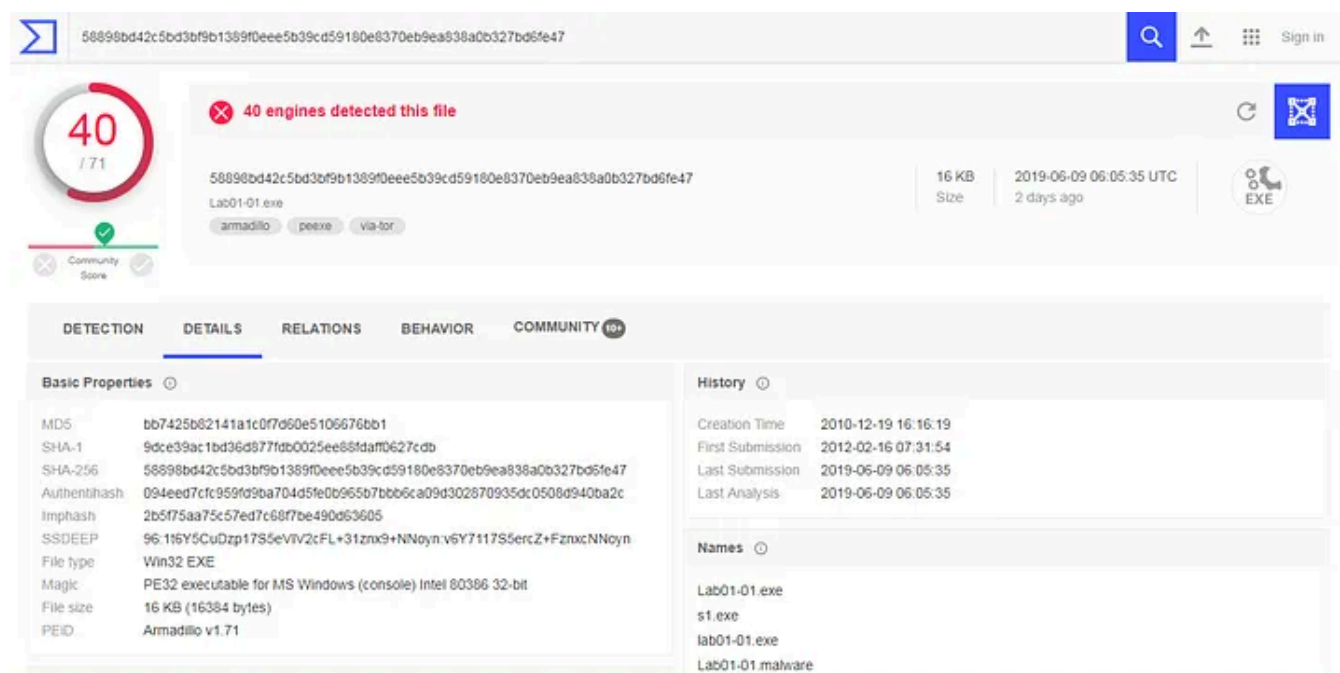
Lab 1-1

This lab uses the files Lab01-01.exe and Lab01-01.dll. Use the tools and techniques described in the chapter to gain information about the files and answer the questions below.

Questions

1. Upload the files to <http://www.VirusTotal.com/> and view the reports. Does either file match any existing antivirus signatures?

Let's upload both of the files on VirusTotal and tally the result!



VirusTotal report for Lab01-01.exe. The file has been detected by 40 engines. The report shows basic properties, history, and names.

Basic Properties

MD5	bb7425b82141a1c0f7d60e5106676bb1
SHA-1	9dce39ac1bd36d977f0025ee86fda0627c0b
SHA-256	58998bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Authenticash	094eed7cfc959fd9ba704d5fe0b965b7bbb6ca09d302870935dc0508d940ba2c
Imphash	2b5f75aa75c57ed7c68f7be490d53605
SSDEEP	96:115Y5CuDzp17S5eVIV2cFL+31zrx9+NNoyN:v5Y7117S5ercZ+FznxcNNoyN
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
File size	16 KB (16384 bytes)
PEID	Armadillo v1.71

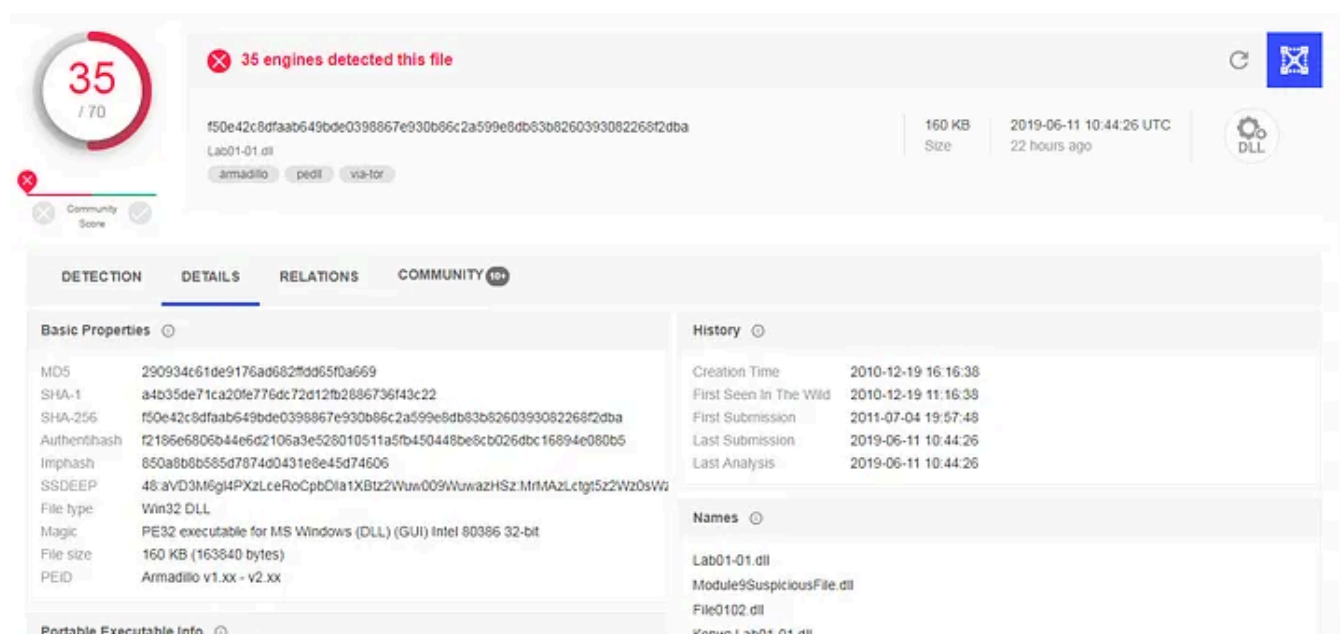
History

Creation Time	2010-12-19 16:16:19
First Submission	2012-02-16 07:31:54
Last Submission	2019-06-09 06:05:35
Last Analysis	2019-06-09 06:05:35

Names

- Lab01-01.exe
- s1.exe
- lab01-01.exe
- Lab01-01.malware

Result of Lab01-01.exe



VirusTotal report for Lab01-01.dll. The file has been detected by 35 engines. The report shows basic properties, history, and names.

Basic Properties

MD5	290934c61de9176a6882fdd65f0a669
SHA-1	a4b35de71ca20fe776dc72d12fb2886736f43c22
SHA-256	f50e42c8dffaab649bde0398867e930b86c2a599e6db83b8260393082268f2dba
Authenticash	f2186e6806b44e6d2106a3e528010511a5fb450448be8cb026dbc16894e080b5
Imphash	850a8b8b555d7874d0431e8e45d74606
SSDEEP	48:avD3M6g4PXPzLcRcPbOlatXBtz2Wuw009WuwazHSz.MrMAZLctgr5z2W20sWz
File type	Win32 DLL
Magic	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
File size	160 KB (163840 bytes)
PEID	Armadillo v1.xx - v2.xx

History

Creation Time	2010-12-19 16:16:38
First Seen In The Wild	2010-12-19 11:16:38
First Submission	2011-07-04 19:57:48
Last Submission	2019-06-11 10:44:26
Last Analysis	2019-06-11 10:44:26

Names

- Lab01-01.dll
- Module9SuspiciousFile.dll
- File102.dll
- Копия Lab01-01.dll

Result of — Lab01-01.dll

We can clearly see that these files have been matched with the previously known signatures and have also been detected as malicious.

2. When were these files compiled?

The compilation time of both file as per the report of VirusTotal is.

Lab01-01.exe → 2010-12-19 16:16:19

Lab01-01.dll → 2010-12-19 16:16:38

We can also find the compilation time using PEview and checking the IMAGE_FILE_HEADER details.

3. Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?

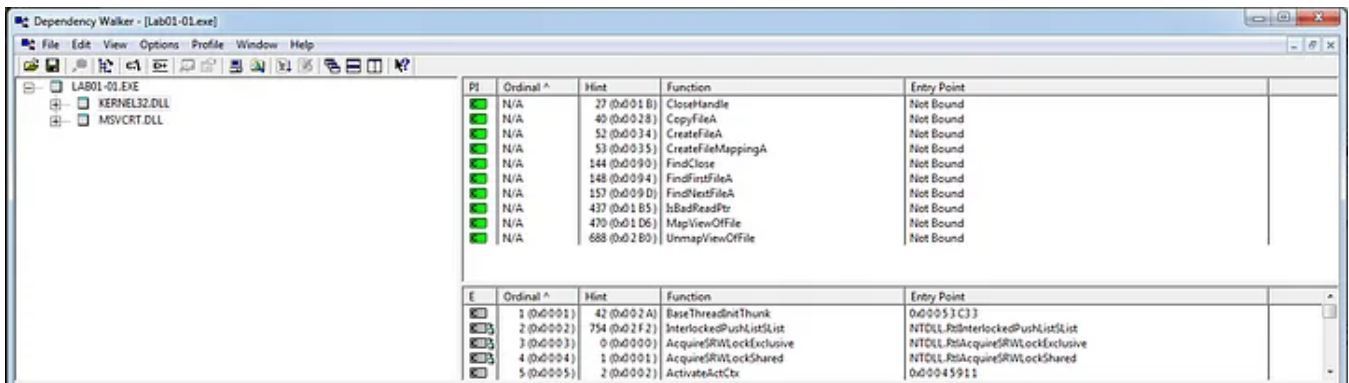
PEiD can be used to find the packed or obfuscated file although we were able to find all the necessary details and the strings. So we conclude that both of these files were not been packed or obfuscated.

4. Do any imports hint at what this malware does? If so, which imports are they?

Both, the executable and DLL file do imports. **Lab01-01.exe** does the following imports.

```
λ strings Lab01-01.exe | grep dll | uniq -u
KERNEL32.dll
MSVCRT.dll
kerne132.dll
kernel32.dll
C:\windows\system32\kerne132.dll
Lab01-01.dll
C:\Windows\System32\Kernel32.dll
```

a. KERNEL32.dll — Following functions from this library were called.



CreateFileA → Creates or opens a file or I/O device.

CopyFileA → Copies an existing file to a new file.

CreateFileMappingA → Creates or opens a named or unnamed file mapping object for a specified file.

FindFirstFileA → Searches a directory for a file or subdirectory with a name that matches a specific name (or partial name if wildcards are used).

FindNextFileA → Continues a file search from a previous call.

MapViewOfFile → Maps a view of a file mapping into the address space of a calling process. Malware can make changes to the actual file once it is mapped.

b. **MSVCRT.dll** → A module containing standard C library functions such as printf, memcpy, and cos. It is a part of the Microsoft C Runtime Library. Non-system processes like **msvcrt.dll** originate from software you installed on your system.

c. **kernel132.dll** → Disguised version of original KERNEL32.DLL.

d. **Lab01-01.dll** → Additional DLL file created for the successful working of Lab01-01.exe executable.

The second file **Lab01-01.dll** do the following imports.

```
C:\Users\Kamran Saifullah\Desktop\Practical M
λ strings Lab01-01.dll | grep dll | uniq -u
KERNEL32.dll
WS2_32.dll
MSVCRT.dll
```

KERNEL32.dll → **Kernel32.dll** is the 32-bit dynamic link library found in the Windows operating system kernel. It handles memory management, input/output operations, and interrupts. When Windows boots up, **kernel32.dll** is loaded into a protected memory space so other applications do not take that space over.

MSVCRT → A module containing standard C library functions such as printf, memcpy, and cos. It is a part of the Microsoft C Runtime Library. Non-system processes like **msvcrt.dll** originate from software you installed on your system.

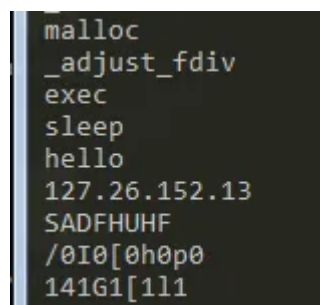
WS2_32.dll → The Windows Sockets Library **ws2_32.dll**, is required by windows and applications to handle network connections.

5. Are there any other files or host-based indicators that you could look for on infected systems?

While finding the strings we found that there is another file named as “Kerne132.dll” which is supposed to be disguised as the “Kernel32.dll”. Also there is another “Lab01-01.DLL” which is not a common OS DLL. So we can look for these files on the system.

6. What network-based indicators could be used to find this malware on infected machines?

We found an IP address when we checked the string. So we capture all the network traffic from all the systems and can look for the communication that is being done over this IP address.



```
malloc
_adjust_fdiv
exec
sleep
hello
127.26.152.13
SADFHUHF
/0I0[0h0p0
141G1[111
```

7. What would you guess is the purpose of these files?

On bringing up all the pieces together we can assume that Lab01-01.exe along with the extension Lab01-01.dll is a malware which creates a backdoor and connects to a C&C server and transfer the critical information. Secondly both of the files are not

packed and Lab01-01.exe searches in and from directories and look for a particular files and replaces them with disguised files. Also it imports functions from core KERNEL32.DLL and network based imports to establish the connections. Also uses the exec function which means that it would be executing some other programs/files along with sleep function which waits until a particular statement or piece of code gets executed. This is mostly used in backdoors.

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



```

.000000..0 080          0000          .000000.          .0          .00
00.
d8P'  `Y8  `"'          `888          d8P'  `Y8b          0888          .dP"'
Y88b
Y88bo.          0000  .00000.  888  0000  888          888  .0000.0  888
]8P'
`"Y88880.  `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'  08880  `Y8bod8P'  08880  08880  `Y8bood8P'  8""888P'  08880  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.

[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




```
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

Qradar101

 Abdelwahab Shandy

CyberDefenders :Qradar101 Blue Team Challenge

Category : Threat Hunting

11 min read · Nov 23, 2023

 4 



http							
No.	Time	Source	Destination	Protocol	Length	Host	Info
13	0.766629967	192.168.126.130	192.168.126.131	HTTP	250	ctld1.windowsupdate.com	GET /n
16	0.779555055	192.168.126.131	192.168.126.130	HTTP	312		HTTP/1
30	2.091895476	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	ctld1.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	ctld1.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	18.497937699	192.168.126.130	192.168.126.131	HTTP	250	ctld1.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



Lists



Staff Picks

630 stories · 920 saves



Stories to Help You Level-Up at Work

19 stories · 581 saves



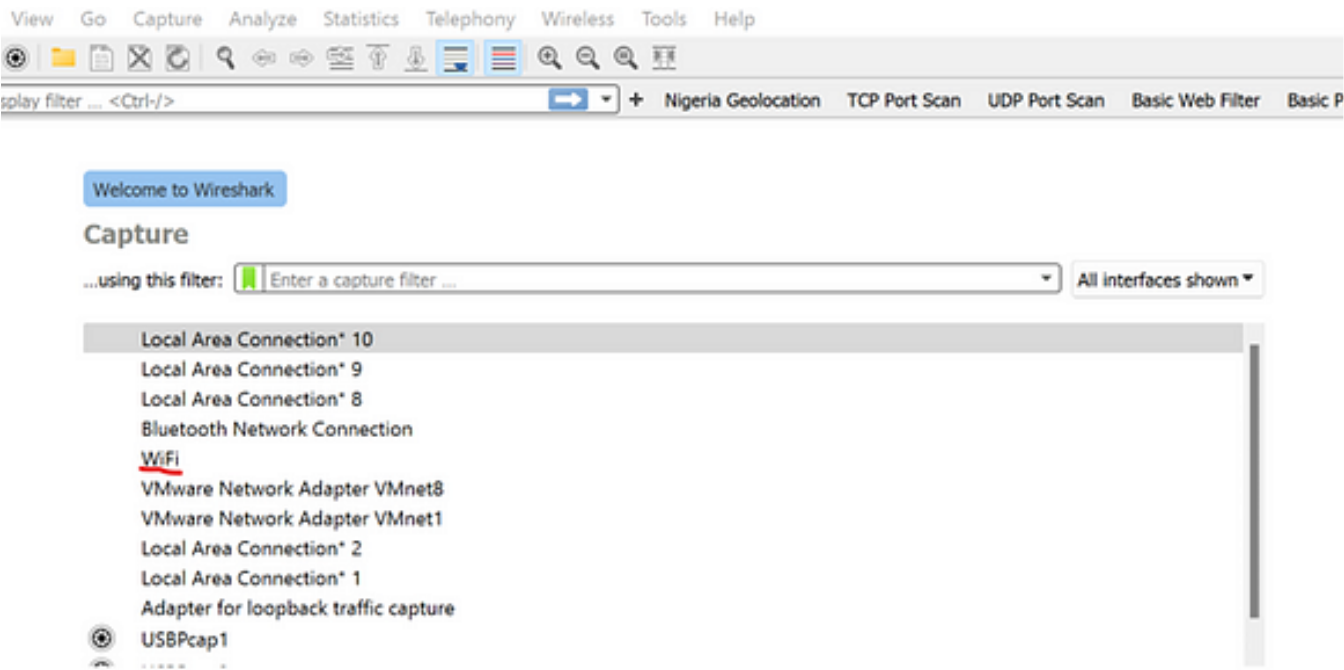
Self-Improvement 101

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



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



```

23 11:53:38 2023 as: nmap -sCV -vvv -oA nmap/exfiltrated 192.168.210.103
63
1 61 (0.27s latency).
  for 111:
reset)
  VERSION
1 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)

3:20:d3:43:b4:c4:8b:cf (RSA)
AAABgQDhPH1/ST7TU3Amq/14c7G+Tm87YbX7Y1smuq17Kpvt18h8MqfK115dW9+za+h6Znago28ewmK+01a436t9Q+2H/Mh4Cm13GrRbpLJk4hChJgCHd5K1LC0KnhXPs/FA3m83
04Mu17w8SwbyyXyji+11eKjQ6Hnje7Kopm5q4U8iJd3LmVME34UMq/qubCUB1aY86A2Mj8mQ1Zqmm3:48eT+Gaub6u15f61DnCCq3zmm37Y3L1UvqAfY1EJ2VhC/Uyr30P8E+Y1D0N6A2Q1
15NqQ2enfPwqt399nigtUerccskdyU06e8XqVmh2CjEYFXIqOn1Aqejr3Ipm8nA31ppd1rXMAmQ1jd508Jxb040R2J8xcFVhfs=
cF0:36:ac:19:d0:8e:73 (ECDSA)
LXwvT11hm1zdhayNTnAAAlbelzdhayNTYAA488816EdIHR7w0eMM8G7CzxbLgub3ump+mb2D3Pe3IXqp/6J83/060De4Ab44nJ8XhJbm/Pzr1YzeJNj60u8lQcG+
cF4:88:8d:33:ce:9b:3a (ED25519)
AAAAIDPC8naIxm8DX1q9tFS+D98m6k8aJEvfq1D3Jr8KZHL
1 Apache httpd 2.4.41 ((Ubuntu))
tries
1/ /panel/ /tmp/

3: 0980083806AE1108548FF82E96385438
ect to http://exfiltrated.offsec/
1 (Ubuntu)

GT 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 110.16 seconds

```



Ardian Danny

[OSCP Practice Series 1] Proving Grounds—Exfiltrated

Machine Type: Linux

3 min read · Dec 26, 2023



Services

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

Dedicated

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 x 7 expert support

Cloud

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 x 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