Open Source Technologies

CA-3

Name: Kummarakuntla Gehini Chandrika

Roll No: 01

Registration Number: 11901601

Course code: Int301

Section: KE022

Question: Using desired Open Source Software trace API calls and behavior of files; give detailed reports;analyze malicious files. Start UniFi Network Controller / Network Application and upgrade/update automatically

To trace Api calls and behaviour of files:

I have used remnux to trace api calls.

Remnux is used for malware analysis. It includes a variety of tools that can be used for tracing API calls in an application. To trace API calls in remnux you can use Strace tool. Strace is a command line tool that is used for tracing system calls and signals made by a program.

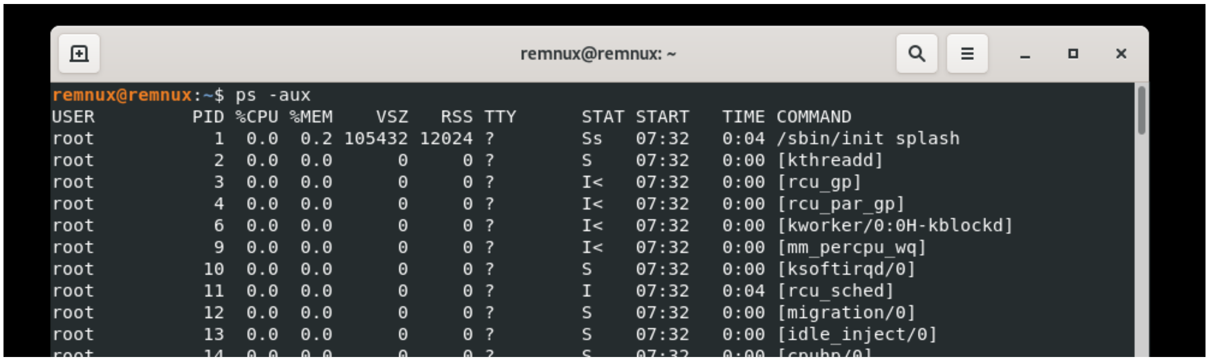
To use the command, first install the command:

sudo apt-get install strace

Identify the pid that you want to trace. To do that you need to type ps- aux to get all the processes that are running in the system.

We are considering to trace the Firefox application. To get the pid of the Firefox application we use pgrep Firefox.

Pic-1.0



```
remnux@remnux:~$ ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.2 105432 12024 ?        Ss   07:32   0:04 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    07:32   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   07:32   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   07:32   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   07:32   0:00 [kworker/0:0H-kblockd]
root           9  0.0  0.0      0     0 ?        I<   07:32   0:00 [mm_percpu_wq]
root          10  0.0  0.0      0     0 ?        S    07:32   0:00 [ksoftirqd/0]
root          11  0.0  0.0      0     0 ?        I    07:32   0:04 [rcu_sched]
root          12  0.0  0.0      0     0 ?        S    07:32   0:00 [migration/0]
root          13  0.0  0.0      0     0 ?        S    07:32   0:00 [idle_inject/0]
root          14  0.0  0.0      0     0 ?        S    07:32   0:00 [cpuhp/0]
```

The pid of the Firefox application is 29680.

Once the process Id is known you should run the strace command using -p to attach to the process.

We have to type:

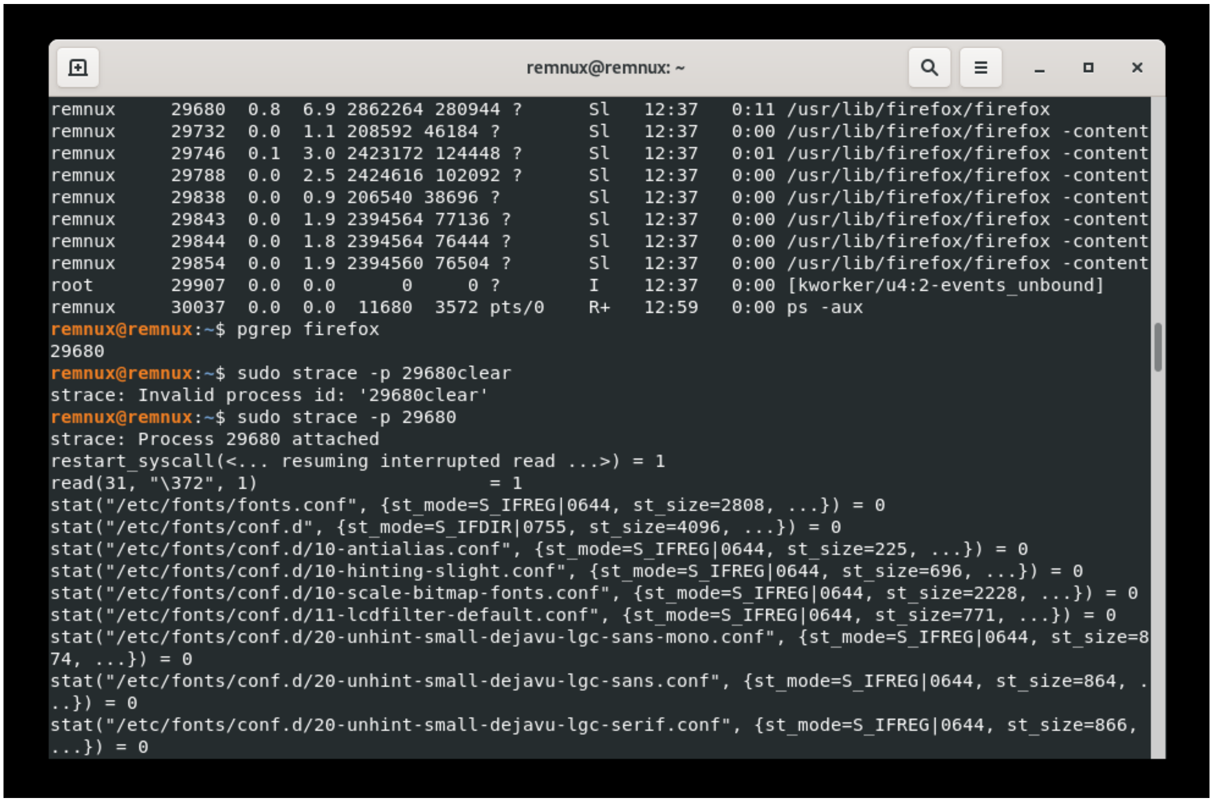
strace -p <pid of the application>

for the firefox it is 29680.

strace -p 29680

when we run this command, the tracing starts and continues till you interrupt or keeps giving the trace data.

Pic-1.1



```
remnux     29680  0.8  6.9 2862264 280944 ?      Sl   12:37   0:11 /usr/lib/firefox/firefox
remnux     29732  0.0  1.1 208592 46184 ?       Sl   12:37   0:00 /usr/lib/firefox/firefox -content
remnux     29746  0.1  3.0 2423172 124448 ?      Sl   12:37   0:01 /usr/lib/firefox/firefox -content
remnux     29788  0.0  2.5 2424616 102092 ?      Sl   12:37   0:00 /usr/lib/firefox/firefox -content
remnux     29838  0.0  0.9 206540 38696 ?       Sl   12:37   0:00 /usr/lib/firefox/firefox -content
remnux     29843  0.0  1.9 2394564 77136 ?      Sl   12:37   0:00 /usr/lib/firefox/firefox -content
remnux     29844  0.0  1.8 2394564 76444 ?      Sl   12:37   0:00 /usr/lib/firefox/firefox -content
remnux     29854  0.0  1.9 2394560 76504 ?      Sl   12:37   0:00 /usr/lib/firefox/firefox -content
root       29907  0.0  0.0      0     0 ?       I    12:37   0:00 [kworker/u4:2-events_unbound]
remnux     30037  0.0  0.0  11680  3572 pts/0    R+   12:59   0:00 ps -aux
remnux@remnux:~$ pgrep firefox
29680
remnux@remnux:~$ sudo strace -p 29680clear
strace: Invalid process id: '29680clear'
remnux@remnux:~$ sudo strace -p 29680
strace: Process 29680 attached
restart_syscall(<... resuming interrupted read ...>) = 1
read(31, "\372", 1)                     = 1
stat("/etc/fonts/fonts.conf", {st_mode=S_IFREG|0644, st_size=2808, ...}) = 0
stat("/etc/fonts/conf.d", {st_mode=S_IFDIR|0755, st_size=4096, ...}) = 0
stat("/etc/fonts/conf.d/10-antialias.conf", {st_mode=S_IFREG|0644, st_size=225, ...}) = 0
stat("/etc/fonts/conf.d/10-hinting-slight.conf", {st_mode=S_IFREG|0644, st_size=696, ...}) = 0
stat("/etc/fonts/conf.d/10-scale-bitmap-fonts.conf", {st_mode=S_IFREG|0644, st_size=2228, ...}) = 0
stat("/etc/fonts/conf.d/11-lcdfilter-default.conf", {st_mode=S_IFREG|0644, st_size=771, ...}) = 0
stat("/etc/fonts/conf.d/20-unhint-small-dejavu-lgc-sans-mono.conf", {st_mode=S_IFREG|0644, st_size=8
74, ...}) = 0
stat("/etc/fonts/conf.d/20-unhint-small-dejavu-lgc-sans.conf", {st_mode=S_IFREG|0644, st_size=864, .
..}) = 0
stat("/etc/fonts/conf.d/20-unhint-small-dejavu-lgc-serif.conf", {st_mode=S_IFREG|0644, st_size=866,
...}) = 0
```

Analyze malicious files

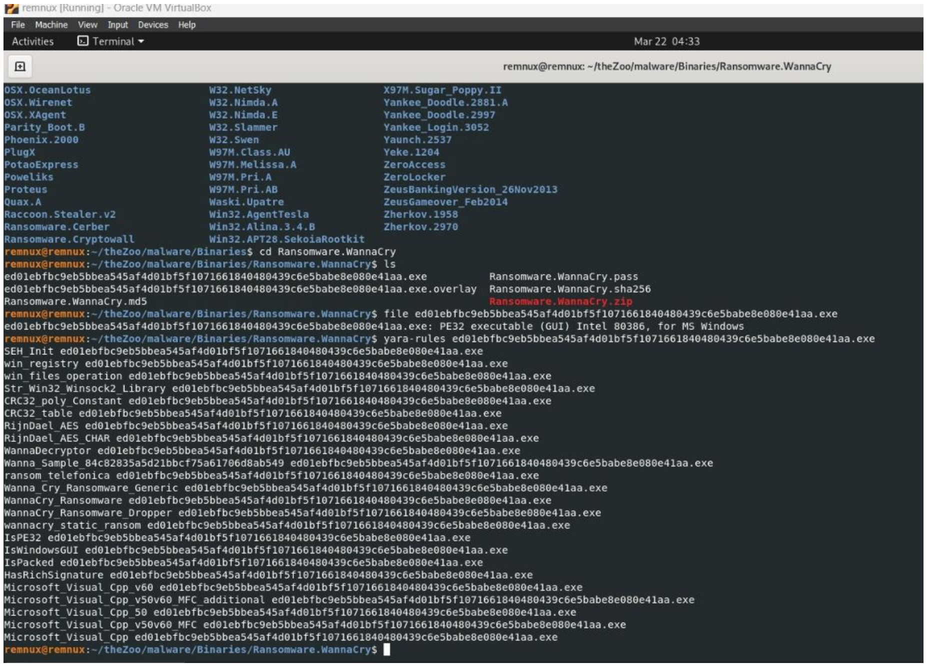
To analyze malicious file, I have used REMnux which is an open-source software.

About REMnux:

REMnux is a Linux-based operating system designed for malware analysis and reverse engineering. It is a lightweight, virtual appliance that comes pre-configured with a variety of powerful tools for analyzing and dissecting malware.

REMnux is built on top of the Ubuntu operating system and is designed to be used as a platform for investigating and analyzing malware in a safe and isolated environment. It includes a range of tools and utilities such as debuggers, disassemblers, memory analysis tools, and network traffic analysis tools that can help security professionals and researchers understand how malware works, identify its behavior, and develop ways to detect and mitigate it.

Pic-2.0


remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mar 22 04:33
remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry

```
OSX.OceanLotus                   W32.NetSky                  X97M.Sugar_Poppy.II
OSX.Wirenet                      W32.Nimda.A                 Yankee_Doodle.2881.A
OSX.XAgent                       W32.Nimda.E                 Yankee_Doodle.2997
Parity_Boot.B                    W32.Slammer                 Yankee_Login.3052
Phoenix.2000                     W32.Swen                    Yaunch.2537
PlugX                            W97M.Class.AU               Yeke.1204
PotaoExpress                     W97M.Melissa.A              ZeroAccess
Poweliks                         W97M.Pri.A                  ZeroLocker
Proteus                          W97M.Pri.AB                 ZeusBankingVersion_26Nov2013
Quax.A                           Waski.Upatre                ZeusGameover_Feb2014
Raccoon.Stealer.v2               Win32.AgentTesla            Zherkov.1958
Ransomware.Cerber                Win32.Alina.3.4.B           Zherkov.2970
Ransomware.Cryptowall            Win32.APT28.SekoiaRootkit
remnux@remnux:~/theZoo/malware/Binaries$ cd Ransomware.WannaCry
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ ls
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe          Ransomware.WannaCry.pass
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe.overlay  Ransomware.WannaCry.sha256
Ransomware.WannaCry.md5                                                       Ransomware.WannaCry.zip
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ file ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe: PE32 executable (GUI) Intel 80386, for MS Windows
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ yara-rules ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
SEH_Init ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
win_registry ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
win_files_operation ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Str_Win32_Winsock2_Library ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
CRC32_poly_Constant ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
CRC32_table ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
RijnDael_AES ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
RijnDael_AES_CHAR ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
WannaDecryptor ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Wanna_Sample_84c82835a5d21bbcf75a61706d8ab549 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
ransom_telefonica ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Wanna_Cry_Ransomware_Generic ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
WannaCry_Ransomware ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
WannaCry_Ransomware_Dropper ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
wannacry_static_ransom ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
IsPE32 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
IsWindowsGUI ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
IsPacked ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
HasRichSignature ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Microsoft_Visual_Cpp_v60 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Microsoft_Visual_Cpp_v50v60_MFC_additional ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Microsoft_Visual_Cpp_50 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Microsoft_Visual_Cpp_v50v60_MFC ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Microsoft_Visual_Cpp ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$
```

The above picture-2.0 shows that :

Let’s take sha256sum value(which is the file name) as sample.exe

Command 1: file sample.exe

It checks whether the file is PE32 executable file or PECompact2 compressed. A PE is a file format developed by Microsoft used for executables (. EXE, . SCR) and dynamic link libraries (. DLL). A PE file infector is a malware family that propagates by appending or wrapping malicious code into other PE files on an infected system.

Command 2: yara-rules sample.exe

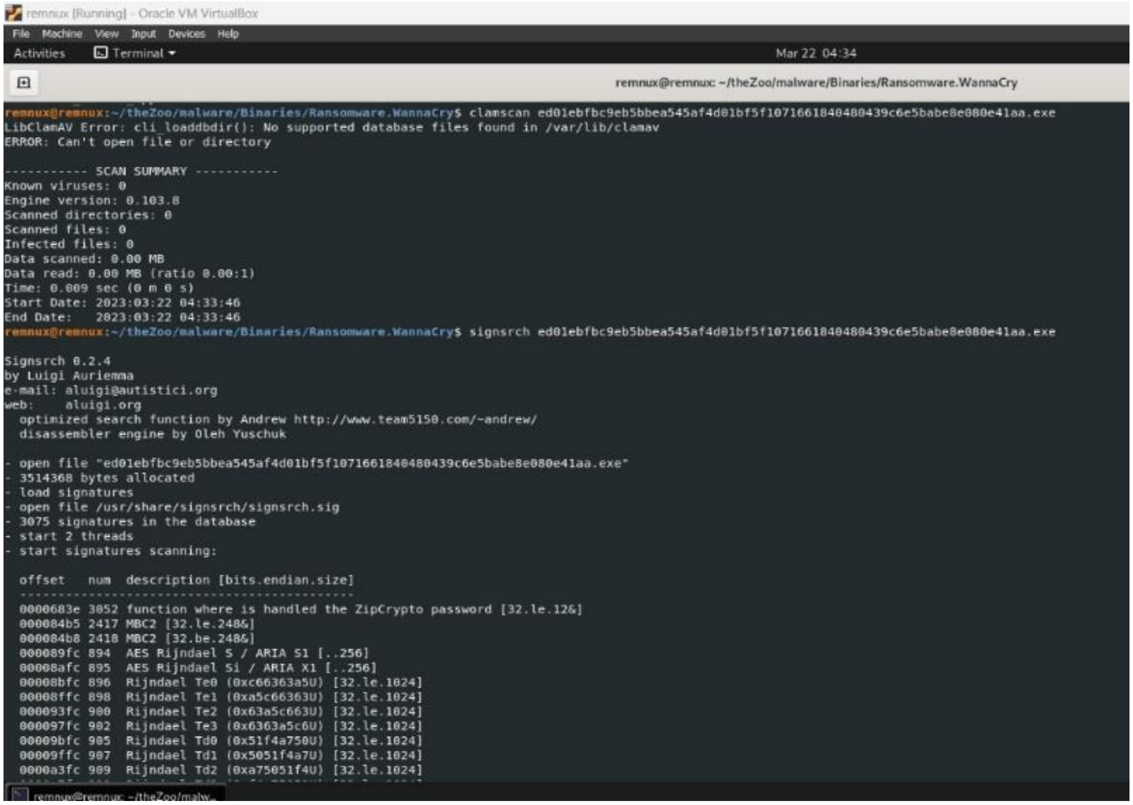
Shows about HTTP, registry, file operations, overlay

YARA is a tool used for identifying and classifying malware based on textual or binary patterns. YARA rules are the rules written in the YARA language to identify patterns of interest in files, processes, or network traffic.

Command-3: clamscan sample.exe

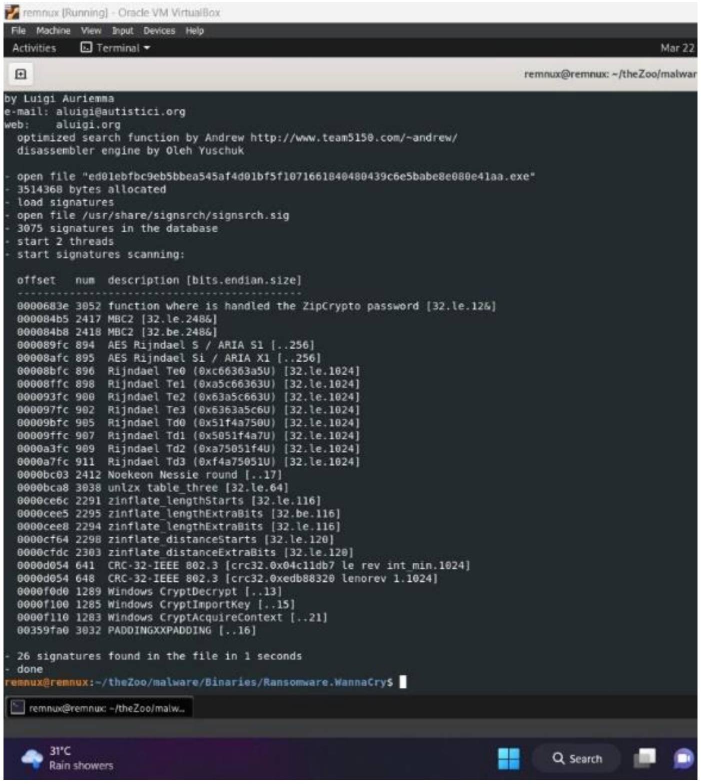
The clamscan command is a command-line antivirus scanner for Linux-based operating systems. It is part of the ClamAV open-source antivirus software package and is used to scan files, directories, and entire filesystems for viruses, malware, and other malicious software.

Pic-2.1


remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mar 22 04:34
remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry

```
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ clamscan ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
LibClamAV Error: cli_loaddbdir(): No supported database files found in /var/lib/clamav
ERROR: Can't open file or directory

----------- SCAN SUMMARY -----------
Known viruses: 0
Engine version: 0.103.8
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.009 sec (0 m 0 s)
Start Date: 2023:03:22 04:33:46
End Date:   2023:03:22 04:33:46
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ signsrch ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

Signsrch 0.2.4
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org
  optimized search function by Andrew http://www.team5150.com/~andrew/
  disassembler engine by Oleh Yuschuk

- open file "ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe"
- 3514368 bytes allocated
- load signatures
- open file /usr/share/signsrch/signsrch.sig
- 3075 signatures in the database
- start 2 threads
- start signatures scanning:

  offset   num  description [bits.endian.size]
  --------------------------------------------
  0000683e 3052 function where is handled the ZipCrypto password [32.le.12&]
  000084b5 2417 MBC2 [32.le.248&]
  000084b8 2418 MBC2 [32.be.248&]
  000089fc 894  AES Rijndael S / ARIA S1 [..256]
  00008afc 895  AES Rijndael Si / ARIA X1 [..256]
  00008bfc 896  Rijndael Te0 (0xc66363a5U) [32.le.1024]
  00008ffc 898  Rijndael Te1 (0xa5c66363U) [32.le.1024]
  000093fc 900  Rijndael Te2 (0x63a5c663U) [32.le.1024]
  000097fc 902  Rijndael Te3 (0x6363a5c6U) [32.le.1024]
  00009bfc 905  Rijndael Td0 (0x51f4a750U) [32.le.1024]
  00009ffc 907  Rijndael Td1 (0x5051f4a7U) [32.le.1024]
  0000a3fc 909  Rijndael Td2 (0xa75051f4U) [32.le.1024]
```

Pic-2.2

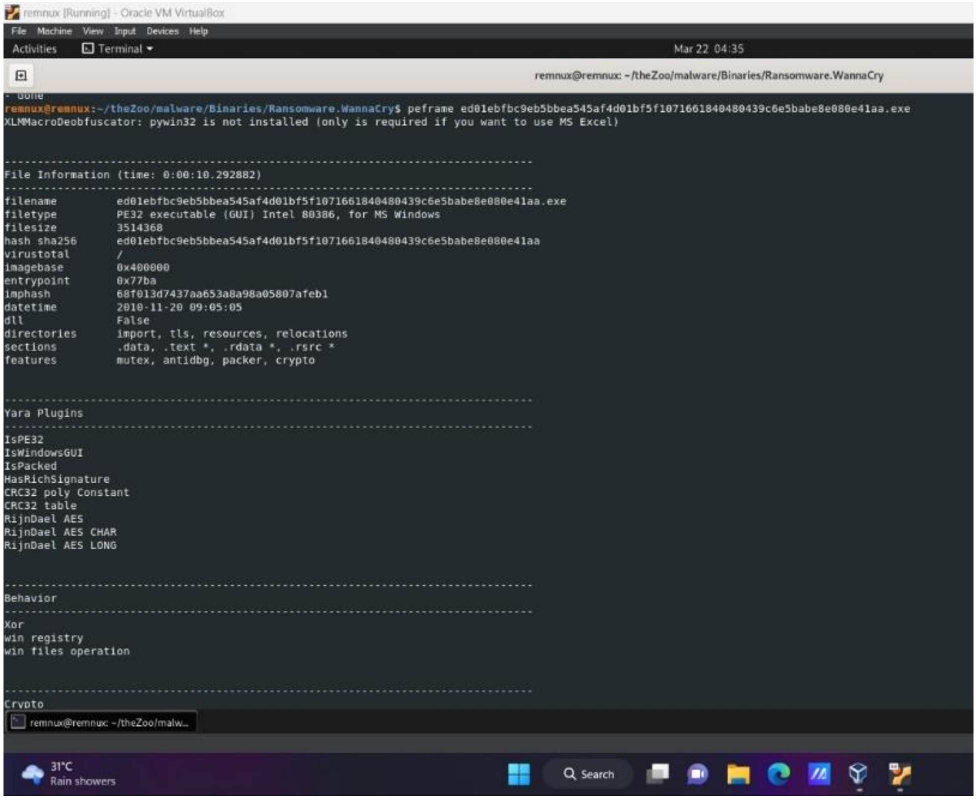

remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mar 22
remnux@remnux: ~/theZoo/malwar
remnux@remnux: ~/theZoo/malw...
31°C
Rain showers
Search

```
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org
  optimized search function by Andrew http://www.team5150.com/~andrew/
  disassembler engine by Oleh Yuschuk

- open file "ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe"
- 3514368 bytes allocated
- load signatures
- open file /usr/share/signsrch/signsrch.sig
- 3075 signatures in the database
- start 2 threads
- start signatures scanning:

  offset   num  description [bits.endian.size]
  --------------------------------------------
  0000683e 3052 function where is handled the ZipCrypto password [32.le.12&]
  000084b5 2417 MBC2 [32.le.248&]
  000084b8 2418 MBC2 [32.be.248&]
  000089fc 894  AES Rijndael S / ARIA S1 [..256]
  00008afc 895  AES Rijndael Si / ARIA X1 [..256]
  00008bfc 896  Rijndael Te0 (0xc66363a5U) [32.le.1024]
  00008ffc 898  Rijndael Te1 (0xa5c66363U) [32.le.1024]
  000093fc 900  Rijndael Te2 (0x63a5c663U) [32.le.1024]
  000097fc 902  Rijndael Te3 (0x6363a5c6U) [32.le.1024]
  00009bfc 905  Rijndael Td0 (0x51f4a750U) [32.le.1024]
  00009ffc 907  Rijndael Td1 (0x5051f4a7U) [32.le.1024]
  0000a3fc 909  Rijndael Td2 (0xa75051f4U) [32.le.1024]
  0000a7fc 911  Rijndael Td3 (0xf4a75051U) [32.le.1024]
  0000bc03 2412 Noekeon Nessie round [..17]
  0000bca8 3038 unlzx table_three [32.le.64]
  0000ce6c 2291 zinflate_lengthStarts [32.le.116]
  0000cee5 2295 zinflate_lengthExtraBits [32.be.116]
  0000cee8 2294 zinflate_lengthExtraBits [32.le.116]
  0000cf64 2298 zinflate_distanceStarts [32.le.120]
  0000cfdc 2303 zinflate_distanceExtraBits [32.le.120]
  0000d054 641  CRC-32-IEEE 802.3 [crc32.0x04c11db7 le rev int_min.1024]
  0000d054 648  CRC-32-IEEE 802.3 [crc32.0xedb88320 lenorev 1.1024]
  0000f0d0 1289 Windows CryptDecrypt [..13]
  0000f100 1285 Windows CryptImportKey [..15]
  0000f110 1283 Windows CryptAcquireContext [..21]
  00359fa0 3032 PADDINGXXPADDING [..16]

- 26 signatures found in the file in 1 seconds
- done
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$
```

Command-4: signsrch sample.exe

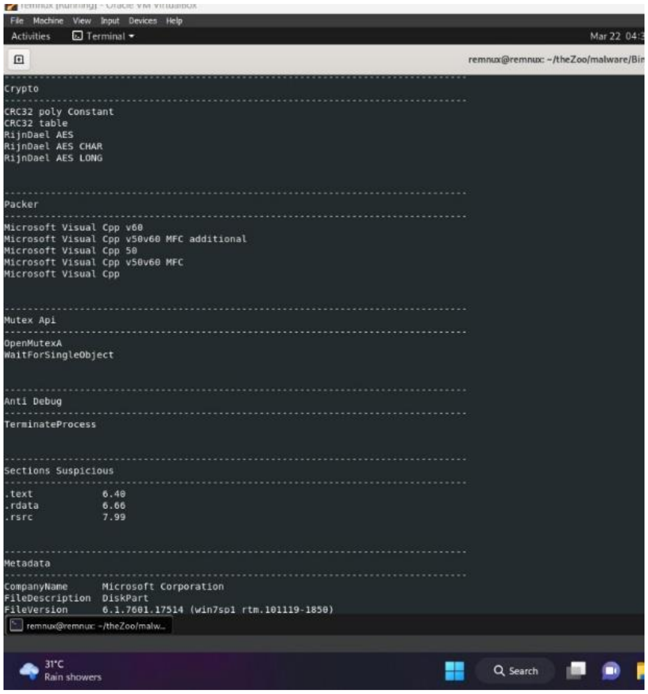
we can verify that the file has been signed using this specific digital signature algorithm.

A digital signature is a cryptographic technique used to ensure the authenticity and integrity of a digital document or file. In the case of executable files, a digital signature can be used to verify that the file has not been tampered with and was signed by a trusted entity.


remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mar 22 04:35
remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry
remnux@remnux: ~/theZoo/malw...
31°C
Rain showers
Search

```
- done
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ peframe ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)


--------------------------------------------------------------------------------
File Information (time: 0:00:10.292882)
--------------------------------------------------------------------------------
filename        ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
filetype        PE32 executable (GUI) Intel 80386, for MS Windows
filesize        3514368
hash sha256     ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
virustotal      /
imagebase       0x400000
entrypoint      0x77ba
imphash         68f013d7437aa653a8a98a05807afeb1
datetime        2010-11-20 09:05:05
dll             False
directories     import, tls, resources, relocations
sections        .data, .text *, .rdata *, .rsrc *
features        mutex, antidbg, packer, crypto


--------------------------------------------------------------------------------
Yara Plugins
--------------------------------------------------------------------------------
IsPE32
IsWindowsGUI
IsPacked
HasRichSignature
CRC32 poly Constant
CRC32 table
RijnDael AES
RijnDael AES CHAR
RijnDael AES LONG


--------------------------------------------------------------------------------
Behavior
--------------------------------------------------------------------------------
Xor
win registry
win files operation


--------------------------------------------------------------------------------
Crypto
```

Pic-2.3


remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mar 22 04:3
remnux@remnux: ~/theZoo/malware/Bin
remnux@remnux: ~/theZoo/malw...
31°C
Rain showers
Search

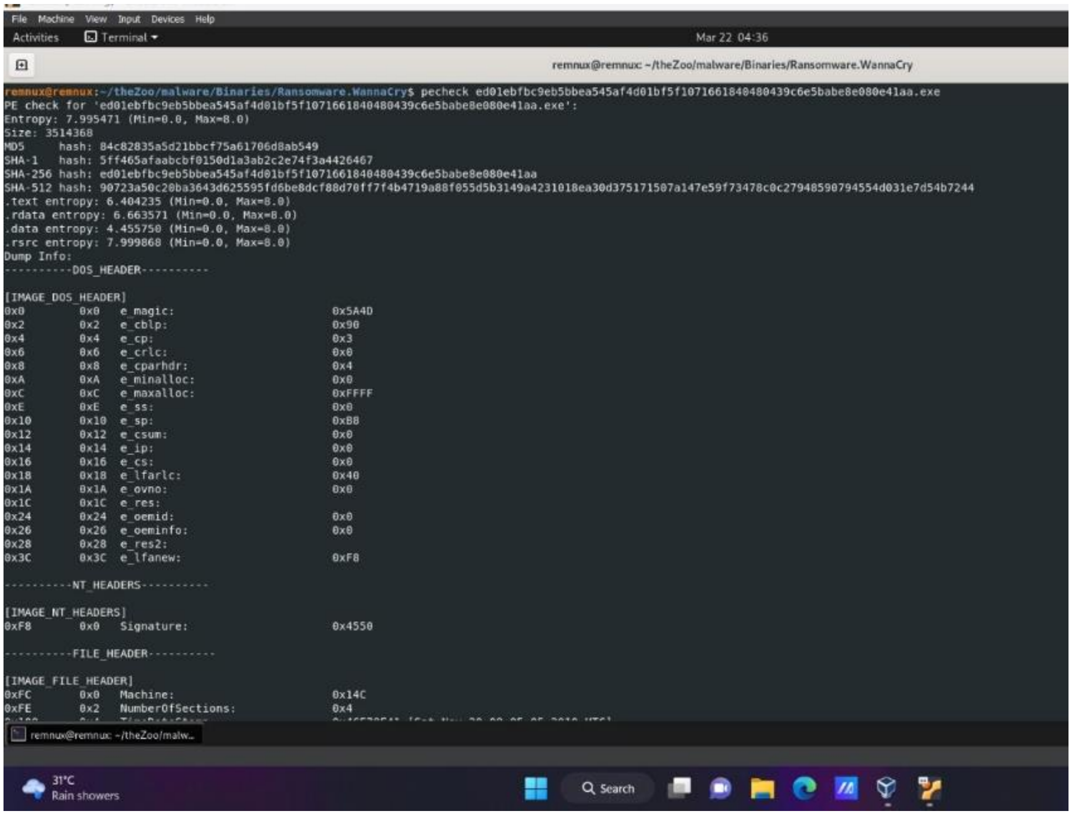
```
--------------------------------------------------------------------------------
Crypto
--------------------------------------------------------------------------------
CRC32 poly Constant
CRC32 table
RijnDael AES
RijnDael AES CHAR
RijnDael AES LONG


--------------------------------------------------------------------------------
Packer
--------------------------------------------------------------------------------
Microsoft Visual Cpp v60
Microsoft Visual Cpp v50v60 MFC additional
Microsoft Visual Cpp 50
Microsoft Visual Cpp v50v60 MFC
Microsoft Visual Cpp


--------------------------------------------------------------------------------
Mutex Api
--------------------------------------------------------------------------------
OpenMutexA
WaitForSingleObject


--------------------------------------------------------------------------------
Anti Debug
--------------------------------------------------------------------------------
TerminateProcess


--------------------------------------------------------------------------------
Sections Suspicious
--------------------------------------------------------------------------------
.text           6.40
.rdata          6.66
.rsrc           7.99


--------------------------------------------------------------------------------
Metadata
--------------------------------------------------------------------------------
CompanyName     Microsoft Corporation
FileDescription DiskPart
FileVersion     6.1.7601.17514 (win7sp1 rtm.101119-1850)
```

Pic-2.4

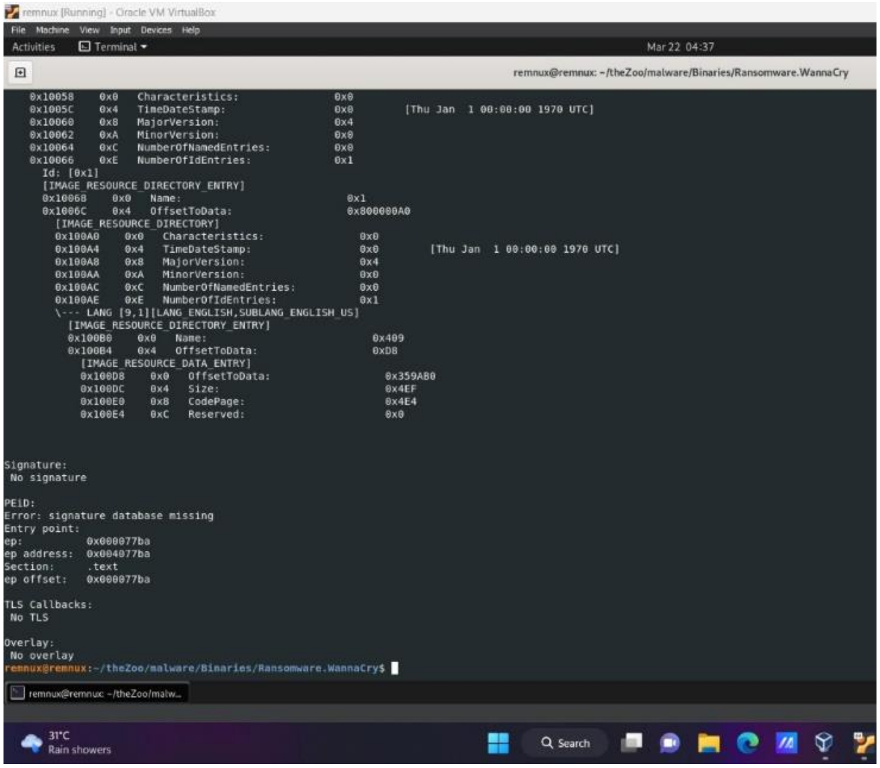
Command-5: peframe sample.exe

It gives output of behaviour of files and clear report , file information,crypto,Hashes, sections code and .rsrc, entropy of .rsrc high, suspicious API references.

Pic-2.5


File Machine View Input Devices Help
Activities
Terminal
Mar 22 04:36
remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry

```
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ pecheck ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
PE check for 'ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe':
Entropy: 7.995471 (Min=0.0, Max=8.0)
Size: 3514368
MD5     hash: 84c82835a5d21bbcf75a61706d8ab549
SHA-1   hash: 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA-256 hash: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA-512 hash: 90723a50c20ba3643d625595fd6be8dcf88d70ff7f4b4719a88f055d5b3149a4231018ea30d375171507a147e59f73478c0c27948590794554d031e7d54b7244
.text entropy: 6.404235 (Min=0.0, Max=8.0)
.rdata entropy: 6.663571 (Min=0.0, Max=8.0)
.data entropy: 4.455750 (Min=0.0, Max=8.0)
.rsrc entropy: 7.999868 (Min=0.0, Max=8.0)
Dump Info:
----------DOS_HEADER----------

[IMAGE_DOS_HEADER]
0x0        0x0   e_magic:                       0x5A4D
0x2        0x2   e_cblp:                        0x90
0x4        0x4   e_cp:                          0x3
0x6        0x6   e_crlc:                        0x0
0x8        0x8   e_cparhdr:                     0x4
0xA        0xA   e_minalloc:                    0x0
0xC        0xC   e_maxalloc:                    0xFFFF
0xE        0xE   e_ss:                          0x0
0x10       0x10  e_sp:                          0xB8
0x12       0x12  e_csum:                        0x0
0x14       0x14  e_ip:                          0x0
0x16       0x16  e_cs:                          0x0
0x18       0x18  e_lfarlc:                      0x40
0x1A       0x1A  e_ovno:                        0x0
0x1C       0x1C  e_res:
0x24       0x24  e_oemid:                       0x0
0x26       0x26  e_oeminfo:                     0x0
0x28       0x28  e_res2:
0x3C       0x3C  e_lfanew:                      0xF8

----------NT_HEADERS----------

[IMAGE_NT_HEADERS]
0xF8       0x0   Signature:                     0x4550

----------FILE_HEADER----------

[IMAGE_FILE_HEADER]
0xFC       0x0   Machine:                       0x14C
0xFE       0x2   NumberOfSections:              0x4
```



remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mar 22 04:37
remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry
remnux@remnux: ~/theZoo/malw...
31°C
Rain showers
Search

```
    0x10058    0x0   Characteristics:              0x0
    0x1005C    0x4   TimeDateStamp:                0x0        [Thu Jan  1 00:00:00 1970 UTC]
    0x10060    0x8   MajorVersion:                 0x4
    0x10062    0xA   MinorVersion:                 0x0
    0x10064    0xC   NumberOfNamedEntries:         0x0
    0x10066    0xE   NumberOfIdEntries:            0x1
      Id: [0x1]
      [IMAGE_RESOURCE_DIRECTORY_ENTRY]
      0x10068    0x0   Name:                         0x1
      0x1006C    0x4   OffsetToData:                 0x800000A0
        [IMAGE_RESOURCE_DIRECTORY]
        0x100A0    0x0   Characteristics:              0x0
        0x100A4    0x4   TimeDateStamp:                0x0        [Thu Jan  1 00:00:00 1970 UTC]
        0x100A8    0x8   MajorVersion:                 0x4
        0x100AA    0xA   MinorVersion:                 0x0
        0x100AC    0xC   NumberOfNamedEntries:         0x0
        0x100AE    0xE   NumberOfIdEntries:            0x1
        \--- LANG [9,1][LANG_ENGLISH,SUBLANG_ENGLISH_US]
          [IMAGE_RESOURCE_DIRECTORY_ENTRY]
          0x100B0    0x0   Name:                         0x409
          0x100B4    0x4   OffsetToData:                 0xD8
            [IMAGE_RESOURCE_DATA_ENTRY]
            0x100D8    0x0   OffsetToData:                 0x359AB0
            0x100DC    0x4   Size:                         0x4EF
            0x100E0    0x8   CodePage:                     0x4E4
            0x100E4    0xC   Reserved:                     0x0


Signature:
 No signature

PEiD:
Error: signature database missing
Entry point:
ep:           0x000077ba
ep address:   0x004077ba
Section:      .text
ep offset:    0x000077ba

TLS Callbacks:
 No TLS

Overlay:
 No overlay
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$
```

Pic-2.6

Command-6: pecheck sample.exe

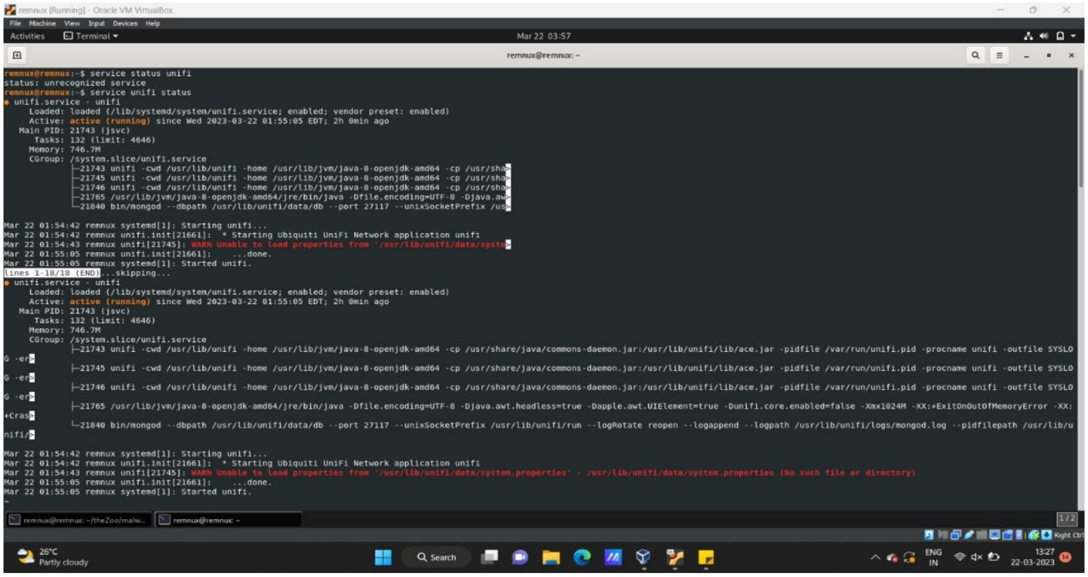
It gives output about Hashes, suspicious API references, overlay.

PECheck is a command-line tool that can be used to verify the PE header and section headers of PE files. It checks the file signature, the size of the image, the entry point, and other information in the PE header. It can also validate the section headers by checking their names, sizes, and attributes.

Unifi Controller:

I have downloaded the unifi controller and upgraded all the devices

The unifi network controller is a free software suite that allows you to set up, configure, manage and analyze your unifi network in a centralized manner.



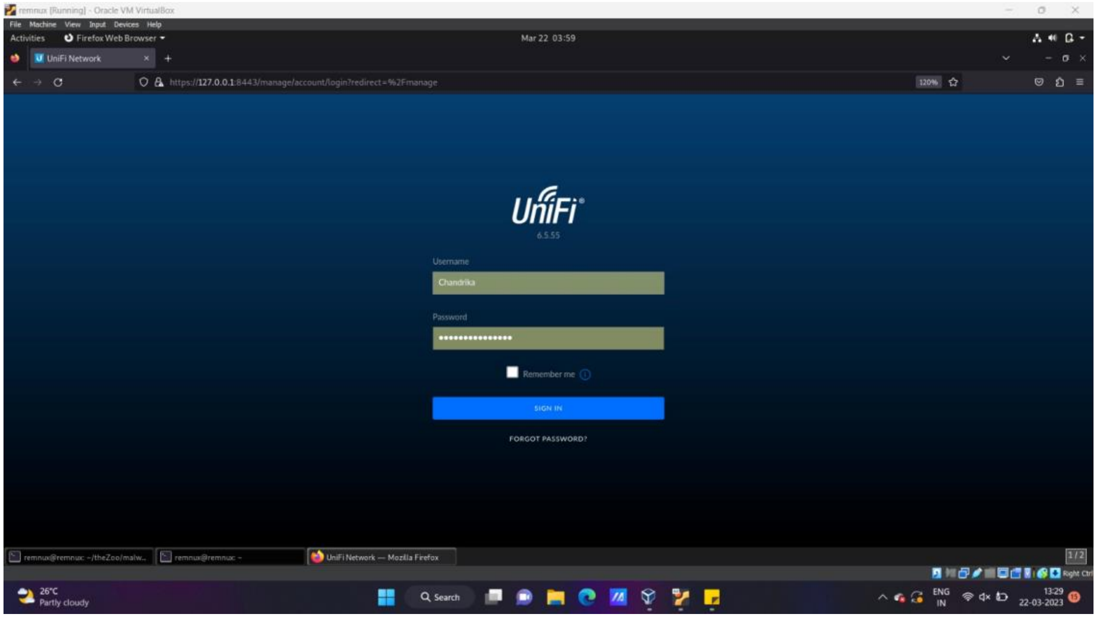
remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Mar 22 03:57
remnux@remnux: ~

```
remnux@remnux:~$ service status unifi
status: unrecognized service
remnux@remnux:~$ service unifi status
● unifi.service - unifi
     Loaded: loaded (/lib/systemd/system/unifi.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-03-22 01:55:05 EDT; 2h 0min ago
   Main PID: 21743 (jsvc)
      Tasks: 132 (limit: 4646)
     Memory: 746.7M
     CGroup: /system.slice/unifi.service
             ├─21743 unifi -cwd /usr/lib/unifi -home /usr/lib/jvm/java-8-openjdk-amd64 -cp /usr/sha>
             ├─21745 unifi -cwd /usr/lib/unifi -home /usr/lib/jvm/java-8-openjdk-amd64 -cp /usr/sha>
             ├─21746 unifi -cwd /usr/lib/unifi -home /usr/lib/jvm/java-8-openjdk-amd64 -cp /usr/sha>
             ├─21765 /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java -Dfile.encoding=UTF-8 -Djava.aw>
             └─21840 bin/mongod --dbpath /usr/lib/unifi/data/db --port 27117 --unixSocketPrefix /us>

Mar 22 01:54:42 remnux systemd[1]: Starting unifi...
Mar 22 01:54:42 remnux unifi.init[21661]:  * Starting Ubiquiti UniFi Network application unifi
Mar 22 01:54:43 remnux unifi[21745]: WARN Unable to load properties from '/usr/lib/unifi/data/syste>
Mar 22 01:55:05 remnux unifi.init[21661]:    ...done.
Mar 22 01:55:05 remnux systemd[1]: Started unifi.
lines 1-18/18 (END)...skipping...
● unifi.service - unifi
     Loaded: loaded (/lib/systemd/system/unifi.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-03-22 01:55:05 EDT; 2h 0min ago
   Main PID: 21743 (jsvc)
      Tasks: 132 (limit: 4646)
     Memory: 746.7M
     CGroup: /system.slice/unifi.service
             ├─21743 unifi -cwd /usr/lib/unifi -home /usr/lib/jvm/java-8-openjdk-amd64 -cp /usr/share/java/commons-daemon.jar:/usr/lib/unifi/lib/ace.jar -pidfile /var/run/unifi.pid -procname unifi -outfile SYSLO
G -er>
             ├─21745 unifi -cwd /usr/lib/unifi -home /usr/lib/jvm/java-8-openjdk-amd64 -cp /usr/share/java/commons-daemon.jar:/usr/lib/unifi/lib/ace.jar -pidfile /var/run/unifi.pid -procname unifi -outfile SYSLO
G -er>
             ├─21746 unifi -cwd /usr/lib/unifi -home /usr/lib/jvm/java-8-openjdk-amd64 -cp /usr/share/java/commons-daemon.jar:/usr/lib/unifi/lib/ace.jar -pidfile /var/run/unifi.pid -procname unifi -outfile SYSLO
G -er>
             ├─21765 /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java -Dfile.encoding=UTF-8 -Djava.awt.headless=true -Dapple.awt.UIElement=true -Dunifi.core.enabled=false -Xmx1024M -XX:+ExitOnOutOfMemoryError -XX:
+Cras>
             └─21840 bin/mongod --dbpath /usr/lib/unifi/data/db --port 27117 --unixSocketPrefix /usr/lib/unifi/run --logRotate reopen --logappend --logpath /usr/lib/unifi/logs/mongod.log --pidfilepath /usr/lib/u
nifi/>

Mar 22 01:54:42 remnux systemd[1]: Starting unifi...
Mar 22 01:54:42 remnux unifi.init[21661]:  * Starting Ubiquiti UniFi Network application unifi
Mar 22 01:54:43 remnux unifi[21745]: WARN Unable to load properties from '/usr/lib/unifi/data/system.properties' - /usr/lib/unifi/data/system.properties (No such file or directory)
Mar 22 01:55:05 remnux unifi.init[21661]:    ...done.
Mar 22 01:55:05 remnux systemd[1]: Started unifi.
~
```

Pic-3.0

The above screen shot(3.1) is about how to check the status of the unifi network controller.

Pic-3.1



remnux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Firefox Web Browser
Mar 22 03:59
UniFi Network
120%
UniFi
6.5.55
Remember me
SIGN IN
FORGOT PASSWORD?
remnux@remnux: ~/theZoo/malw...
remnux@remnux: ~
UniFi Network — Mozilla Firefox
1 / 2
Right Ctrl
26°C
Partly cloudy
Search
ENG
IN
13:29
22-03-2023

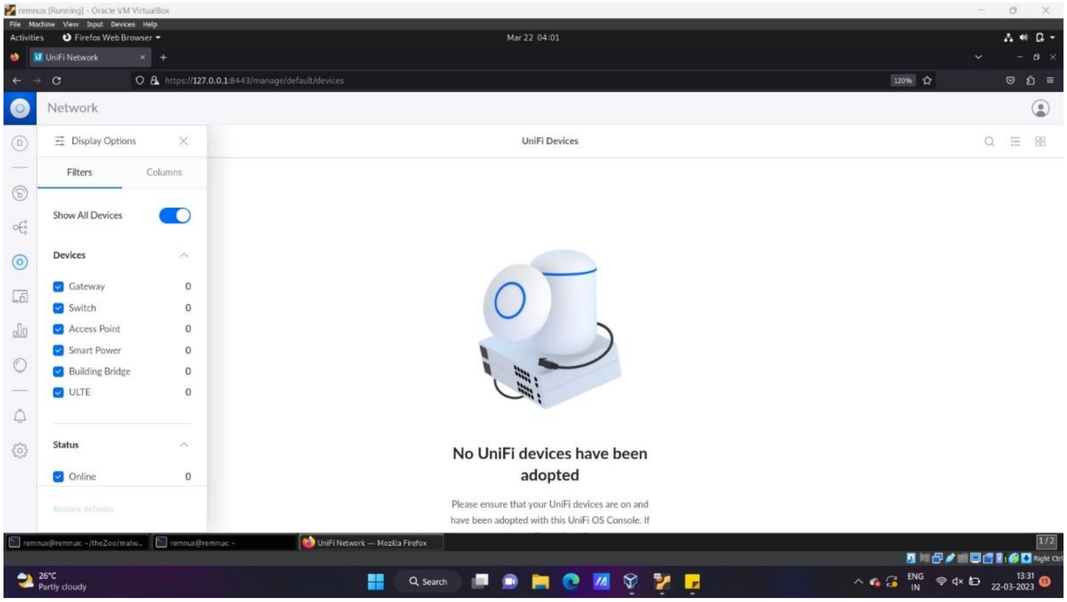
https://127.0.0.1:8443/manage/account/login?redirect=%2Fmanage

Username
Chandrika

Password
•••••••••••••••

The above picture – 3.1 shows the login page of the unifi controller.In order to login we have to create an account in unifi controller. Inorder to open this we have use the url “https://127.0.0.1:8443/manage/account/login?redirect=%2Fmanage”

Pic-3.2



Show All Devices

Devices

☑ Gateway	0
☑ Switch	0
☑ Access Point	0
☑ Smart Power	0
☑ Building Bridge	0
☑ ULTE	0

Status

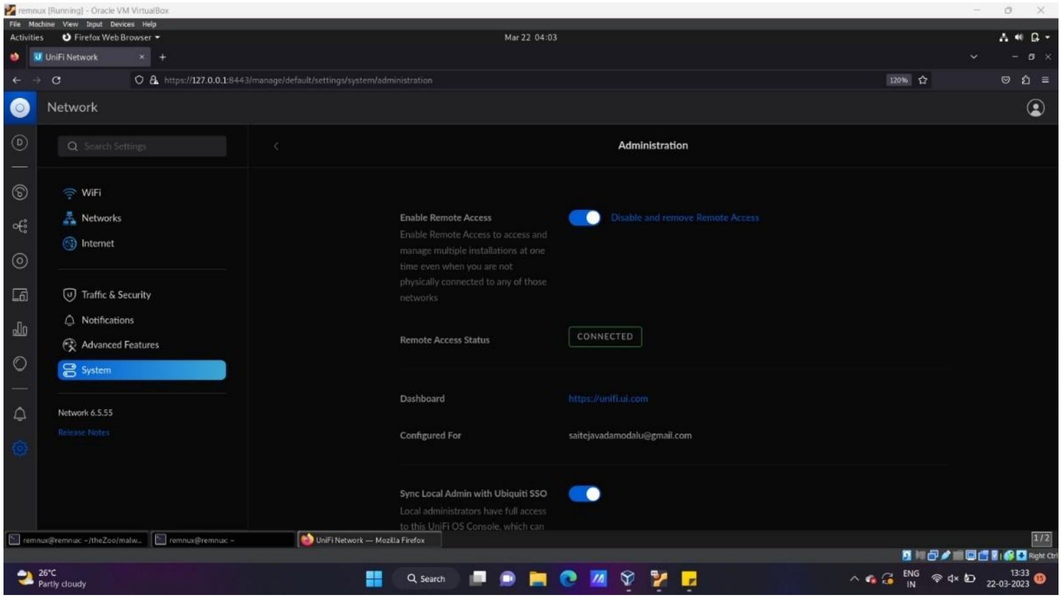
☑ Online	0

No UniFi devices have been adopted

Please ensure that your UniFi devices are on and have been adopted with this UniFi OS Console. If

The above picture - 3.2 shows the available unifi devices in the unifi network. As I have no unifi devices which are adopted, I took the available devices.

Pic-3.3



Enable Remote Access — Disable and remove Remote Access

Enable Remote Access to access and manage multiple installations at one time even when you are not physically connected to any of those networks

Remote Access Status: CONNECTED

Dashboard: https://unifi.ui.com

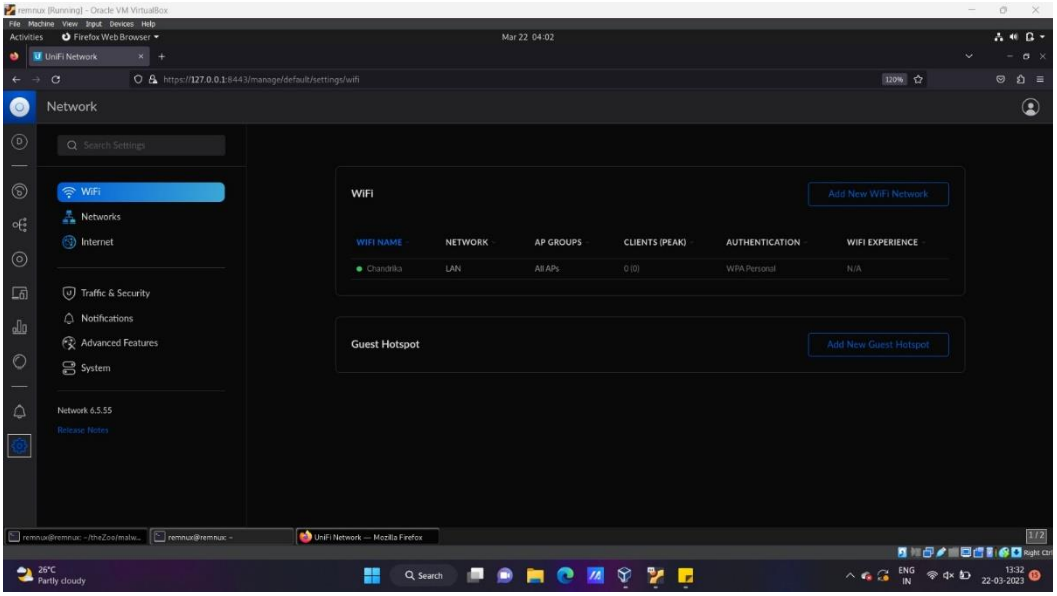
Configured For: saitejavadamodalu@gmail.com

Sync Local Admin with Ubiquiti SSO

Local administrators have full access to this UniFi OS Console, which can

The above picture - 3.3 shows the remote access status as connected. Remote access is to access and manage multiple installations at one time even when you are not physically connected to any networks.

pic-3.4



https://127.0.0.1:8443/manage/default/settings/wifi

WiFi

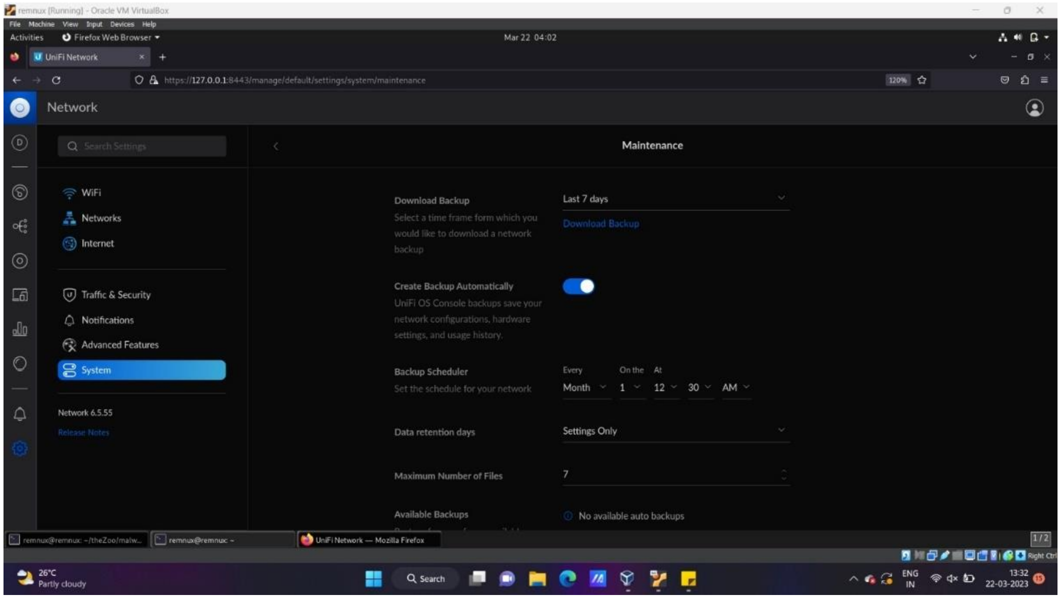
WIFI NAME	NETWORK	AP GROUPS	CLIENTS (PEAK)	AUTHENTICATION	WIFI EXPERIENCE
● Chandrika	LAN	All APs	0 (0)	WPA Personal	N/A

Guest Hotspot

Network 6.5.55

The above picture 3-4 shows that the user “Chandrika” is connected to which type of network.

Pic-3.5



https://127.0.0.1:8443/manage/default/settings/system/maintenance

Maintenance

Download Backup
Select a time frame form which you would like to download a network backup
Last 7 days

Create Backup Automatically
UniFi OS Console backups save your network configurations, hardware settings, and usage history.

Backup Scheduler
Set the schedule for your network
Every Month, On the 1, At 12 30 AM

Data retention days: Settings Only

Maximum Number of Files: 7

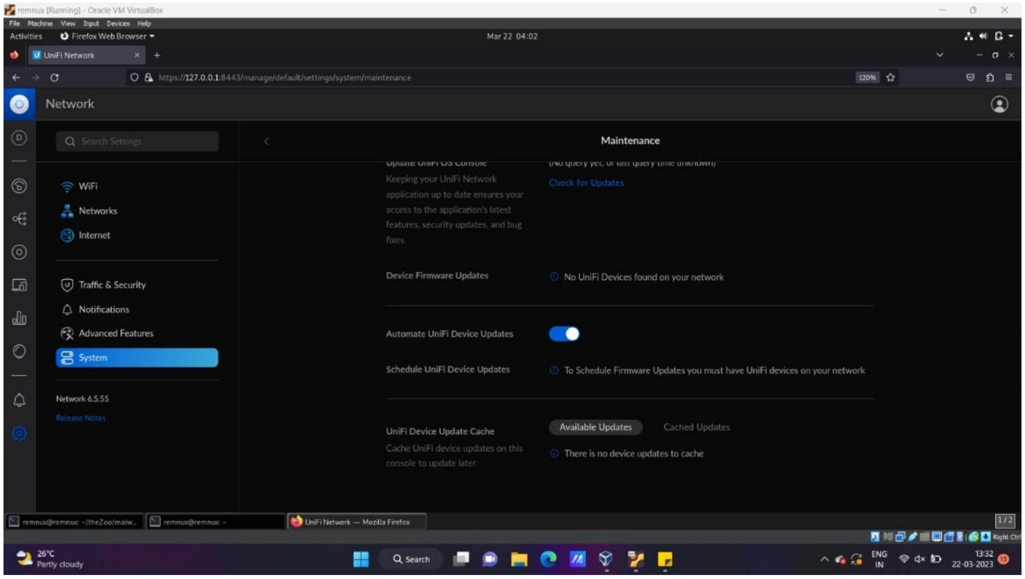
Available Backups: No available auto backups

Network 6.5.55

The above picture-3.5 shows how to create backup automatically. Unifi os console backps save your network configuration hardware settings and usage history. We can also download the backup.

To do backup automatically go to settings -> system -> create backup automatically -> enable

Pic-3.6



Maintenance

Update UniFi OS Console — (No query yet, or last query time unknown)

Keeping your UniFi Network application up to date ensures your access to the application's latest features, security updates, and bug fixes.

Check for Updates

Device Firmware Updates — No UniFi Devices found on your network

Automate UniFi Device Updates — ●

Schedule UniFi Device Updates — To Schedule Firmware Updates you must have UniFi devices on your network

UniFi Device Update Cache — Available Updates | Cached Updates

Cache UniFi device updates on this console to update later.

There is no device updates to cache

The main task of this part of the project is to make the devices automatically upgrade or update. As there are no unifi devices have been adopted, I have used the available devices in the unifi network controller.

The above picture-3.5 shows how to enable the automatic updates for the unifi devices. To enable the option we have to go to settings -> system -> automatic unifi devices update -> enable.

Github:

https://github.com/Chandrika1302/OpenSourceCA3