

Open Source Technologies

Name:-Yoshita Peddi

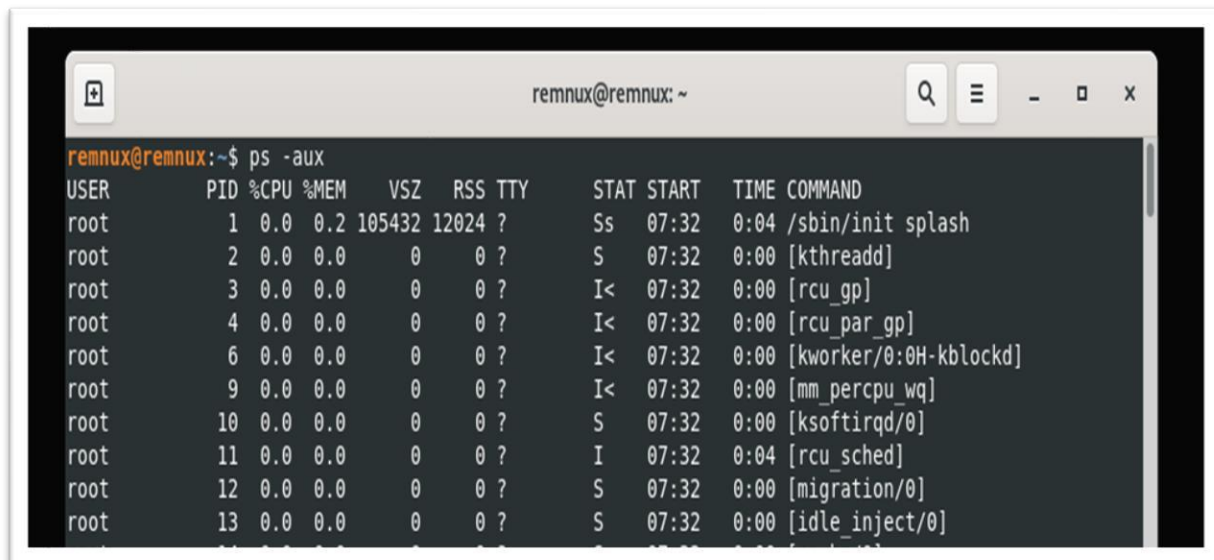
Roll.No:-01

Reg.No:-11901355

Course Code:-INT301

Section:-KE059

Fig-1

A terminal window titled 'remnux@remnux: ~' with standard window controls. The command 'ps -aux' has been executed, displaying a table of system processes. The table includes columns for USER, PID, %CPU, %MEM, VSZ, RSS, TTY, STAT, START, TIME, and COMMAND. The output lists several system processes running as root, including /sbin/init splash, [kthreadd], [rcu_gp], [rcu_par_gp], [kworker/0:0H-kblockd], [mm_percpu_wq], [ksoftirqd/0], [rcu_sched], [migration/0], and [idle_inject/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]
```

Fig-1.1

```

remnux@remnux: ~
remnux 29680 0.8 6.9 2862264 280944 ? S 12:37 0:11 /usr/lib/firefox/firefox
remnux 29732 0.0 1.1 208592 46184 ? S 12:37 0:00 /usr/lib/firefox/firefox -content
remnux 29746 0.1 3.0 2423172 124448 ? S 12:37 0:01 /usr/lib/firefox/firefox -content
remnux 29788 0.0 2.5 2424616 102092 ? S 12:37 0:00 /usr/lib/firefox/firefox -content
remnux 29838 0.0 0.9 206540 38696 ? S 12:37 0:00 /usr/lib/firefox/firefox -content
remnux 29843 0.0 1.9 2394564 77136 ? S 12:37 0:00 /usr/lib/firefox/firefox -content
remnux 29844 0.0 1.8 2394564 76444 ? S 12:37 0:00 /usr/lib/firefox/firefox -content
remnux 29854 0.0 1.9 2394560 76504 ? S 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=874, ...}) = 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

```

Fig-2.0

```

remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry
ls
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe Ransomware.WannaCry.pass
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe.overlay Ransomware.WannaCry.sha256
Ransomware.WannaCry.md5 Ransomware.WannaCry.zip
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe PE32 executable (GUI) Intel 80386, for MS Windows
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe: EH Init
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe in registry
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe in files operation
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe tr Win32_Winsock2_Library
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe RC32_poly_Constant
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe RC32_table
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe l3jn0ael_AES
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe l3jn0ael_AES_CHAR
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe annaDecryptor
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe anna_Sample
B4c82835a5d21bbc75a61706d8ab549 d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe anna_telefonica
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe anna_Cry_Ransomware_Generic
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe annaCry_Ransomware
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe annaCry_Ransomware_Dropper
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe annaCry_Ransomware_Static
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe sPE32
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe sWindowsGUI
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe sPacked
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe sRichSignature
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe icrosoft_Visual_Cpp_v60
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe icrosoft_Visual_Cpp_v50v60_MFC_additional
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe icrosoft_Visual_Cpp_v50
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe icrosoft_Visual_Cpp_v50v60_MFC
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe icrosoft_Visual_Cpp
d01ebfbc9eb5bba545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

```

Fig-2.1

```

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
canned directories: 0
canned 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.126]
000084b5 2417 MBC2 [32.le.2486]
000084b8 2418 MBC2 [32.be.2486]
000089fc 894 AES Rijndael S / ARIA S1 [..256]
00008afc 895 AES Rijndael S1 / 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]

```

Fig-2.2

```

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.126]
000084b5 2417 MBC2 [32.le.2486]
000084b8 2418 MBC2 [32.be.2486]
000089fc 894 AES Rijndael S / ARIA S1 [..256]
00008afc 895 AES Rijndael S1 / 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]
0000b0c3 2412 Noekeon Hessian round [..17]
0000b0ca 3038 unLzx table three [32.le.64]
0000ce6c 2291 inflate.lengthStarts [32.le.116]
0000cee5 2295 inflate.lengthExtraBits [32.be.116]
0000cee8 2294 inflate.lengthExtraBits [32.le.116]
0000cf64 2298 inflate.distanceStarts [32.le.120]
0000cfdc 2303 inflate.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 PADDINGXXXPadding [..16]

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

```

Fig-2.3

```

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/malware/Binaries/Ransomware.WannaCry$ peframe ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
LMacroDeobfuscator: 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, antidebug, 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
-----
remnux@remnux: ~/theZoo/malw...

```

Fig-2.4

```

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

-----
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)

remnux@remnux: ~/theZoo/malw...

```


Fig-2.5

```

remnux@remnux: ~/theZoo/malware/Binaries/Ransomware.WannaCry
remnux@remnux:~/theZoo/malware/Binaries/Ransomware.WannaCry$ pecheck ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
E check for 'ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe':
ntropy: 7.995471 (Min=0.0, Max=8.0)
Size: 3514368
DOS hash: 84c82035a5d21bbc775a61706d8ab549
HA-1 hash: 5f4f45f9aabc9f0150d1a3ab2c2e74f3a4426467
HA-256 hash: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
HA-512 hash: 90723a50c20ba3643d625595fd6be8dcf88d70ff7f4b4719a88f655d5b3149a4231018ea30d375171507a147e59f73478c0c27948590794554d031e7d54b7244
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]
x0 0x0 e_magic: 0x5A4D
x2 0x2 e_cblp: 0x90
x4 0x4 e_cp: 0x3
x6 0x6 e_crc16: 0x0
x8 0x8 e_cpardr: 0x4
xA 0xA e_minalloc: 0x0
xC 0xC e_maxalloc: 0xFFFF
xE 0xE e_ss: 0x0
x10 0x10 e_sp: 0xBB
x12 0x12 e_csum: 0x0
x14 0x14 e_ip: 0x0
x16 0x16 e_cs: 0x0
x18 0x18 e_lfarlc: 0x40
x1A 0x1A e_ovno: 0x0
x1C 0x1C e_res:
x24 0x24 e_oemid: 0x0
x26 0x26 e_oeminfo: 0x0
x28 0x28 e_res2:
x3C 0x3C e_lfanew: 0xF8
-----NT_HEADERS-----
[IMAGE_NT_HEADERS]
x78 0x0 Signature: 0x4550
-----FILE_HEADER-----
[IMAGE_FILE_HEADER]
x7C 0x0 Machine: 0x14C
x7E 0x2 NumberOfSections: 0x4

```

Fig-2.6

```

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 (java)
Tasks: 132 (limit: 4946)
Memory: 746.7M
CGroup: /system.slice/unifi.service
└─21743 unifi -cld /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 SYSLOG
└─21745 unifi -cld /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 SYSLOG
└─21746 unifi -cld /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 SYSLOG
└─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:
└─21840 bin/nongod --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/unifi/

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]: WNM unable to load properties from /usr/lib/unifi/data/system
Mar 22 01:55:05 remnux unifi.init[21661]: ...done.
Mar 22 01:55:05 remnux systemd[1]: Started unifi.
lines 1-13/100 (100) --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 (java)
Tasks: 132 (limit: 4946)
Memory: 746.7M
CGroup: /system.slice/unifi.service
└─21743 unifi -cld /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 SYSLOG
└─21745 unifi -cld /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 SYSLOG
└─21746 unifi -cld /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 SYSLOG
└─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:
└─21840 bin/nongod --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/unifi/

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]: WNM 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.

```

Fig-3.0

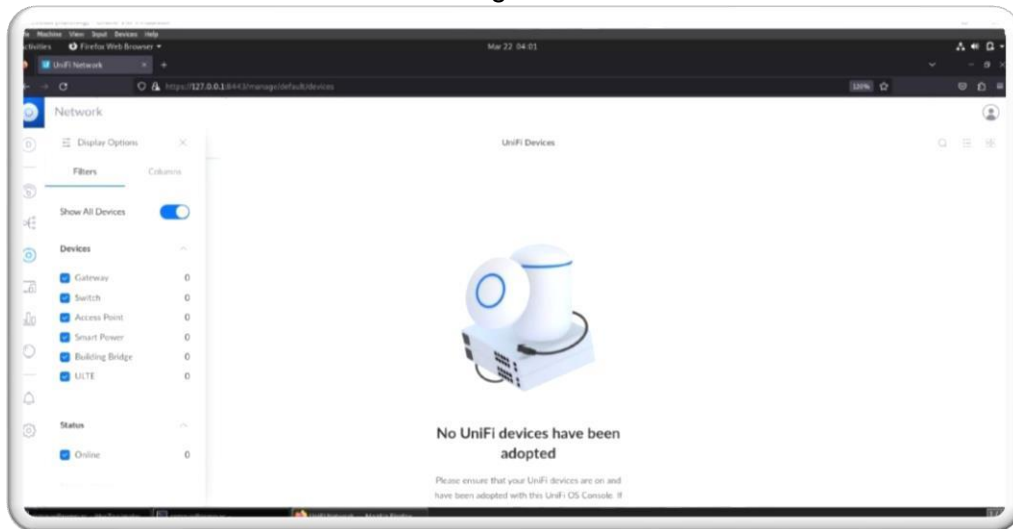


Fig-3.1

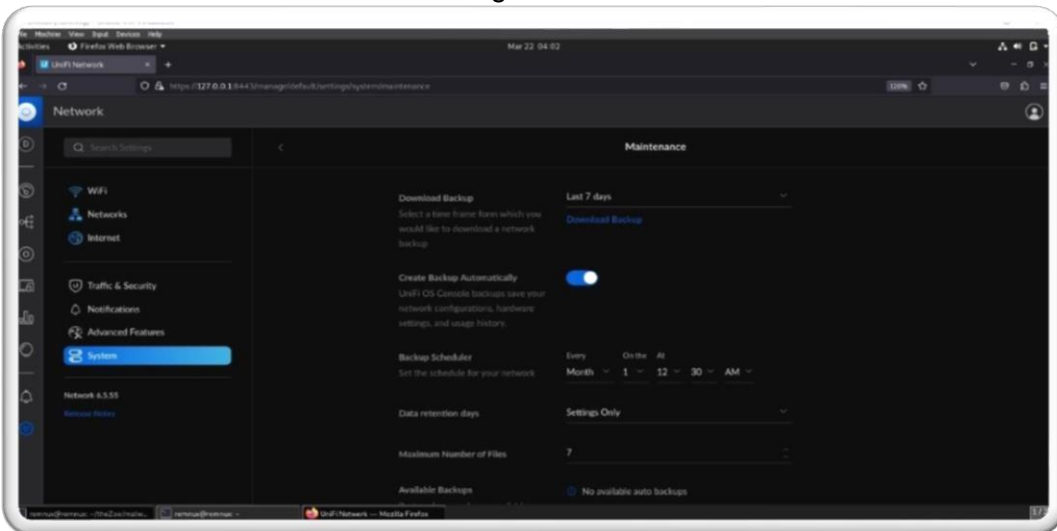


Fig-3.2

