

Đăng nhập



Thảo luận » Virus/Malware

Hướng dẫn rà soát phần mềm độc hại trên Linux











Trên Windows, có rất nhiều phần mềm cũng như giải pháp để phát hiện và ngăn chặn phần mềm độc hại. Tuy nhiên, trên các phiên bản phân phối của Linux, dường như có ít các giải pháp để phát hiện và ngăn chặn chúng. Vì vậy trong bài viết này, mình sẽ hướng dẫn các bạn cách rà soát phần mềm độc hại bằng các công cụ có sẵn trên Linux.

Các chương trình độc hại thường có mục đích cụ thể. Để đạt được mục đích này, malware cần thực hiện một số hoạt động cụ thể, chính những hoạt động này để lại dấu vết trên hệ thống, từ đó giúp chúng ta có thể điều tra và phát hiện chúng.

Các biểu hiện thường thấy ở phần mềm độc hại là:

- Nghe trên một hoặc một số cổng xác định hoặc giao tiếp với máy chủ kiểm soát và ra lệnh (C2)
- Tăng mức tiêu thụ tài nguyên máy tính như RAM, CPU, băng thông mạng...

Rà soát phần mềm độc hại

1. Kiểm tra mức độ tiêu tốn tài nguyên

Để kiểm tra tiến trình nào tiêu tốn tài nguyên hệ thống như CPU, RAM, chúng ta sử dụng lệnh: top

(5)						kali@kali -				- • *
File Actions Edit								0/40		
top - 01:55:26 up 31 min, 1 user, load average: 0.12, 0.06, 0.06										
Tasks: 187 total, 1 running, 186 sleeping, 0 stopped, 0 zombie %Cpu(s): 0.2 us, 0.2 sy, 0.0 ni, 99.6 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st										
MiB Mem										5.8 buff/cache
MiB Swap	o:	975.0 to	otal	, 975	.0 free,	0	0.0	used.	119	5.8 avail Mem
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+ COMMAND
	root			1259984		45832	31/11/12	0.7	8.3	0:17.65 Xorg
	kali			10132	4020	3272		0.7	0.2	0:09.16 top
	root		0	23644	6952	4220		0.3	0.3	0:00.51 systemd-udevd
	root		0	162724	6872	5932		0.3	0.3	0:06.97 vmtoolsd
834	root	20	0	1412076	42992	24684	s	0.3	2.1	0:02.87 containerd
1444	kali	20	0	289228	36732	28804	S	0.3	1.8	0:06.66 vmtoolsd
1594	kali	20	0	1275920	83920	66216	S	0.3	4.1	0:08.71 qterminal
1922	root	20	0	0	0	0	Ι	0.3	0.0	0:00.53 kworker/2:3-mpt_+
1	root	20	0	163964	10444	7832	S	0.0	0.5	0:02.83 systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.01 kthreadd
3	root	0	-20	0	0	0	Ι	0.0	0.0	0:00.00 rcu_gp
4	root	0	-20	0	0	0	Ι	0.0	0.0	0:00.00 rcu_par_gp
6	root	0	-20	0	0	0	Ι	0.0	0.0	0:00.00 kworker/0:0H-eve+
8	root	0	-20	0	0	0	Ι	0.0	0.0	0:00.00 mm_percpu_wq
9	root	20	0	0	0	0	S	0.0	0.0	0:00.00 rcu_tasks_rude_
10	root	20	0	0	0	0	S	0.0	0.0	0:00.00 rcu_tasks_trace
11	root	20	0	0	0	0	S	0.0	0.0	0:00.05 ksoftirqd/0
12	root	20	0	0	0	0	Ι	0.0	0.0	0:00.72 rcu_sched
13	root	rt	0	0	0	0	S	0.0	0.0	0:00.05 migration/0
13	root	rt	0	0	0	0	S	0.0	0.0	

Ở đây, chúng ta kiểm tra xem tiến trình nào sử dụng nhiều CPU, RAM và các tên các tiến trình đáng ngờ.

Khi tìm thấy tiến trình đáng ngờ, bạn có thể xem thông tin chi tiết bằng lệnh:

Để kết thúc tiến trình đáng ngờ, bạn dùng lệnh:

kill -9 pid_tiến trình

2. Kiểm tra mức sử dụng ổ đĩa

Để kiểm tra mức độ sử dụng ổ đĩa, chúng ta dùng công cụ *iotop*.

Actions Edit	View Help		NAMES AND A		
otal Di	ISK READ:	0.00 B/s Total D	ISK WRITE:	0	.00 B/s
ırrent	DISK READ:	0.00 B/s Current	DISK WRITE:	0	.00 B/s
TID	PRIO USER	DISK READ DISK WRI	TE SWAPIN	10>	COMMAND
1	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % i	nit splash
2	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [kthreadd]
3	be/0 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [rcu_gp]
4	be/0 root	0.00 B/s 0.00 B	/s 0.00 % (0.00 % [rcu_par_gp]
6	be/0 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [kworker/0:0H-events_highpri]
8	be/0 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [mm_percpu_wq]
9	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [rcu_tasks_rude_]
10	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [rcu_tasks_trace]
11	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [ksoftirqd/0]
12	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [rcu_sched]
13	rt/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [migration/0]
15	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [cpuhp/0]
16	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [cpuhp/1]
17	rt/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [migration/1]
18	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [ksoftirqd/1]
20	be/0 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [kworker/1:0H-events_highpri]
21	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [cpuhp/2]
22	rt/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [migration/2]
23	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [ksoftirqd/2]
25	be/0 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [kworker/2:0H-events_highpri]
26	be/4 root	0.00 B/s 0.00 B	/s 0.00 %	0.00 % [cpuhp/3]
keys:	any: refresh	g: quit <u>i</u> : ionice	o: active p	: procs	<u>a</u> : accum
sort:	r: asc <u>left</u> :	SWAPIN right: COMMA	ND <u>home</u> : TI	D <u>end</u> :	COMMAND

Để xem tiến trình nào đọc và ghi từ ổ đĩa trong mỗi 25 giây, ta dùng lệnh sudo pidstat -dl 25

```
(kali⊕kali)-[~]
  -$ <u>sudo</u> pidstat -dl 25
Linux 5.10.0-kali7-amd64 (kali)
                                          02/13/2022
                                                                            (4 CPU)
                                                           _x86_64_
02:08:40 AM
              UID
                         PID
                               kB_rd/s
                                          kB_wr/s kB_ccwr/s iodelay
                                                                      Command
02:09:05 AM
                                                                       jbd2/sda1-8
02:09:05 AM
                                            10.71
02:09:05 AM
                                                                      /usr/sbin/NetworkManager --no-daemon
02:09:05 AM
                                                                      /usr/sbin/rsyslogd -n -iNONE
                         513
02:09:05 AM
                                                                       kworker/2:3-events
```

3. Kiểm tra các cổng mở

Phần mềm độc hại thường sẽ chạy trên một cổng nhất định, cố gắng mở cổng và thiết lập kết nối. Để xem các kết nối được thiết lập, ta dùng lệnh *sudo ss -tupn*



Khi thấy một kết nối đáng ngờ, chúng ta có thể chặn chúng bằng cách sử dụng iptables.

Để xem trạng thái của các cổng đang mở, chúng ta dùng lệnh sudo ss -tulpn



4. Phân tích cách tệp được mở

Để xem các tệp nào được mở có liên kết với một tiến trình cụ thể, chúng ta dùng lệnh *sudo Isof* | *grep* tên tiến trình



5. Kiểm tra các dịch vụ đang chạy

Để kiểm tra các dịch vụ đang chạy, chúng ta dùng lệnh systemctl list-unit-files | grep active

6. Tìm các tệp được tạo gần đây

Phần mềm độc hại thường tạo ra một số tệp trên hệ thống cho một mục đích nhất định, chúng ta có thể tìm các tệp được tạo gần đây với lệnh find.

Ví dụ, để tìm các tệp được tạo trong 50 ngày trong thư mục , ta dùng lệnh find /bin/ -mtime -50

```
(kali⊕ kali)-[~]
 -$ find /bin/ -mtime -50
/bin/
/bin/msf-hmac_sha1_crack
/bin/msf-java_deserializer
/bin/msf-jsobfu
/bin/msf-nasm_shell
/bin/msf-virustotal
/bin/msf-metasm shell
/bin/msf-pattern_create
/bin/msf-makeiplist
/bin/msf-find badchars
/bin/msf-msf_irb_shell
/bin/msf-md5_lookup
/bin/msf-exe2vbs
/bin/msf-pdf2xdp
/bin/msf-egghunter
/bin/msf-exe2vba
/bin/msf-halflm_second
/bin/msf-pattern_offset
```

Để xem tất cả các tệp được truy cập trong 50 ngày, ta dùng lệnh find / -atime 50

Để tìm các thuộc tính (permission, owner, group) đã bị thay đổi trong 50 phút trước đó, ta dùng lệnh find / - cmin -50

Để tìm tất cả các tệp đã được truy cập trong 60 phút trước đó, ta dùng lệnh find / -amin -60

7. Kiểm tra các dịch vụ chạy cùng với hệ thống khi khởi động

Phần mềm độc hại sẽ cố gắng tồn tại bền bỉ trên hệ thống, do đó, nó thường tìm cách khởi chạy cùng với hệ thống khi khởi động. Để kiểm tra các dịch vụ tự động chạy khi hệ thống khởi động, ta dùng lệnh

systemctl list-unit-files | grep enabled

Systemctl list-unit-files grep enabled run-vmblock\x2dfuse.mount enabled en			
run-vmblock\x2dfuse.mount binfmt-support.service cnabled console-setup.service cnabled consoled			
binfmt-support.service console-setup.service console-setup.service conservice			onablad
console-setup.service enabled enabled cron.service enabled cron.service enabled enabled cron.service enabled enabled enabled docker.service enabled enabled enabled estyme.service enabled ena			
cron.service docker.service enabled en			
docker.service enabled enabled disabled getty@.service enabled enabled enabled disabled getty@.service enabled enabled enabled haveged.service enabled enabled enabled keyboard-setup.service enabled enabled enabled lightdm.service enabled enabled enabled enabled modemManager.service enabled ena			
e2scrub_reap.service enabled disabled getty@.service enabled enabled enabled haveged.service enabled enabled enabled enabled enabled lightdm.service enabled enabled enabled lightdm.service enabled enabled enabled enabled networking.service enabled enable			
getty@.service enabled enabled enabled keyboard-setup.service enabled enabled lightdm.service enabled enabled enabled enabled lightdm.service enabled			
haveged.service keyboard-setup.service lightdm.service ModemManager.service networking.service networking.service NetworkManager-dispatcher.service NetworkManager-wait-online.service NetworkManager.service nembled NetworkManager.service nembled networkManager.service nembled networkManager.service nembled nembled networkManager.service nembled			The state of the s
keyboard-setup.service lightdm.service modemManager.service metworking.service networkManager-dispatcher.service NetworkManager-wait-online.service NetworkManager.service networkManager.service networkManager-wait-online.service networkManager.service neabled networkManager.service neabled networkManager.service neabled networkManager.service neabled networkManager.service neabled neabled nesservice neabled neabled neabled neabled neabled nesservice neabled	<u> </u>		
lightdm.service enabled disabled ModemManager.service enabled enabled enabled networking.service enabled enabled enabled enabled NetworkManager-dispatcher.service enabled disabled NetworkManager-wait-online.service enabled enabled enabled nfs-common.service enabled enabled enabled enabled enabled open-vm-tools.service enabled enabled enabled ersync.service enabled enabled enabled enabled enabled enabled systemd-fsck-root.service enabled enabled enabled systemd-fsck-root.service enabled enabled enabled systemd-pstore.service enabled enabled enabled systemd-pstore.service enabled enabled enabled systemd-pstore.service enabled enabled enabled enabled systemd-pstore.service enabled enabled enabled enabled enabled enabled enabled enabled systemd-pstore.service enabled			
ModemManager.serviceenabledenablednetworking.serviceenabledenabledNetworkManager-dispatcher.serviceenableddisabledNetworkManager.serviceenabledenablednfs-common.servicemaskedenabledopen-vm-tools.serviceenabledenabledrsync.serviceenabledenabledrsyslog.serviceenabledenabledsmartmontools.servicedisabledenabledsmartmontools.serviceenabledenabledsudo.servicemaskedenabledsystemd-fsck-root.serviceenabled-runtimedisabledsystemd-networkd.servicedisabledenabledsystemd-pstore.serviceenabledenabled			THE SECOND SECON
networking.serviceenabledenabledNetworkManager-dispatcher.serviceenableddisabledNetworkManager-wait-online.serviceenableddisabledNetworkManager.serviceenabledenablednfs-common.servicemaskedenabledopen-vm-tools.serviceenabledenabledrsync.serviceenabledenabledrsyslog.serviceenabledenabledsmartmontools.servicedisabledenabledsudo.serviceenabledenabledsystemd-fsck-root.serviceenabledenabledsystemd-networkd.servicedisabledenabledsystemd-pstore.serviceenabledenabled			
NetworkManager-dispatcher.service enabled disabled NetworkManager-wait-online.service enabled smartmontools.service disabled enabled enabled swartmontools.service enabled enabled enabled systemd-fsck-root.service enabled enabled enabled systemd-networkd.service disabled enabled systemd-pstore.service enabled			enabled
NetworkManager-wait-online.service NetworkManager.service nfs-common.service open-vm-tools.service rsync.service rsyslog.service rtkit-daemon.service smartmontools.service sudo.service systemd-fsck-root.service systemd-pstore.service systemd-pstore.service systemd-pstore.service enabled disabled enabled			
NetworkManager.service enabled enabled open-vm-tools.service masked enabled smartmontools.service disabled enabled enabled swartmontools.service enabled enabled enabled enabled systemd-fsck-root.service enabled enabled enabled systemd-networkd.service disabled enabled enabled systemd-pstore.service enabled enabled enabled enabled			
nfs-common.service masked enabled open-vm-tools.service enabled enabled rsync.service enabled enabled enabled rsyslog.service enabled enabled enabled enabled enabled enabled smartmontools.service enabled enabled sudo.service masked enabled systemd-fsck-root.service enabled enabled systemd-networkd.service disabled enabled systemd-pstore.service enabled enabled enabled enabled			
open-vm-tools.service enabled enabled rsync.service enabled enabled enabled rsyslog.service enabled enabled enabled rtkit-daemon.service disabled enabled smartmontools.service enabled enabled sudo.service masked enabled systemd-fsck-root.service enabled enabled systemd-networkd.service disabled enabled systemd-pstore.service enabled enabled enabled		enapted	A CONTRACTOR OF THE CONTRACTOR
rsync.service enabled enabled rsyslog.service enabled enabled enabled rtkit-daemon.service disabled enabled enabled smartmontools.service enabled enabled sudo.service masked enabled systemd-fsck-root.service enabled enabled systemd-networkd.service disabled enabled systemd-pstore.service enabled enabled enabled		masked	
rsyslog.service enabled enabled rtkit-daemon.service disabled enabled smartmontools.service enabled enabled sudo.service masked enabled systemd-fsck-root.service enabled enabled systemd-networkd.service disabled enabled systemd-pstore.service enabled enabled enabled			enabled
rtkit-daemon.service disabled enabled smartmontools.service enabled enabled sudo.service masked enabled systemd-fsck-root.service enabled-runtime disabled systemd-networkd.service disabled enabled systemd-pstore.service enabled enabled			enabled
smartmontools.serviceenabledenabledsudo.servicemaskedenabledsystemd-fsck-root.serviceenabled-runtimedisabledsystemd-networkd.servicedisabledenabledsystemd-pstore.serviceenabledenabled			enabled
sudo.servicemaskedenabledsystemd-fsck-root.serviceenabled-runtimedisabledsystemd-networkd.servicedisabledenabledsystemd-pstore.serviceenabledenabled			enabled
systemd-fsck-root.service enabled-runtime disabled systemd-networkd.service disabled enabled systemd-pstore.service enabled enabled			enabled
systemd-networkd.service disabled enabled systemd-pstore.service enabled enabled			enabled
systemd-pstore.service enabled enabled			AND CONTRACTOR OF THE PARTY OF
			enabled
			THE RESIDENCE OF THE PARTY OF T
	systemd-remount-fs.service		
systemd-resolved.service disabled enabled			4.00
docker.socket enabled enabled	docker.socket	enabled	enabled

8. Kiểm tra Cron job.

Để tránh sự phát hiện, phần mềm độc hại thường lập lịch để chạy một tác vụ nào đó trong khoảng thời gian xác định. Để đạt được điều này, malware thường sử dụng cron. Để kiểm tra tất cả các tác vụ đã được lập lịch cho tất cả user trên hệ , ta dùng lệnh $for\ user\ in\ (cut-f1-d:/etc/passwd); dosudocrontab-uuser -l 2>/dev/null | <math>grep\ -v'$ "; done

9. Kiểm tra các tập lệnh được thực thi tự động

Linux có nhiều tập lệnh chạy tự động khi user đăng nhập vào hệ thống. Phần mềm độc hại lợi dụng tính năng này để tự động khởi chạy. Do đó, chúng ta cần rà soát các tệp và thư mục như

- /etc/profile
- /etc/profile.d/*
- ~/.bash profile
- ~/,bashrc
- /etc/bashrc

Chỉnh sửa lần cuối bởi người điều hành: 25/02/2022

Mời các bạn tham gia Group WhiteHat để thảo luận và cập nhật tin tức an ninh mạng hàng ngày. Lưu ý từ WhiteHat: Kiến thức an ninh mạng để phòng chống, không làm điều xấu. Luật pháp liên quan

mattcilus



Lam Trường

ok nha ad

Mời các bạn tham gia Group WhiteHat để thảo luận và cập nhật tin tức an ninh mạng hàng ngày. Lưu ý từ WhiteHat: Kiến thức an ninh mạng để phòng chống, không làm điều xấu. Luật pháp liên quan

Mũ Nồi

Bài viết rất hữu ích cám ơn admin

Mời các bạn tham gia Group WhiteHat để thảo luận và cập nhật tin tức an ninh mạng hàng ngày. Lưu ý từ WhiteHat: Kiến thức an ninh mạng để phòng chống, không làm điều xấu. Luật pháp liên quan



@ 2009 - 2023 Bkav Corporation

Bạn phải đăng nhập hoặc đăng ký để phản hồi tại đây.

Chuyên mục

Bài yiết liên quan

WarGame

Hướng dẫn phân tích extension trình duyệt độc hại với ExtAnalysis

Thảo luận

() 15/05/2022 · ○ 0

Video

Hướng dẫn xử lý các lỗi của hệ thống phát sinh do mã độc

Số người đạng 5/03/2022 ng kệ - White Hat Forum

Tòa nhà HH1, Khu đô thị Yên Hòa, Cầu Giấy, Hà Nội

Giấy phép MXH số 355 GP - BITT do BITT cấp

Ghi rõ 'nguồn Bkav' khi phát hành lại thông tin từ Website này

[Tool Re 2] Hướng dẫn debug động virus bằng IDA

③ 10/09/2021 · Ø 1

[Tool Re 1] Hướng dẫn debug động virus bằng IDA

() 03/08/2021 · **(**) 0

Xin hướng dẫn giải mã dữ liệu bị đổi sang đuôi .mpal

③ 09/06/2020 · **反** 1