# 虚拟货币"挖矿"自查参考方法

广东工业大学

网络信息与现代教育技术中心

2022年3月

一、自查	
Linux 系统	3
1、Pwnrig 挖矿	3
2、PhoenixMiner 挖矿	3
3、.font-unix 挖矿	3
4、伪装 python 程序挖矿	4
Windows 系统	5
webminer 挖矿	5
1、安装杀毒软件修复系统漏洞和打补丁	5
2、关闭高危漏洞	5
3、修复第三方软件漏洞	6
二、常用处理	6
1、及时隔离主机	6
2、阻断异常网络通信	6
3、清除定时任务	7
4、清除启动项	7
5、清除预加载 so	8
6、清除 ssh 公钥	8
7、清除挖矿木马	8
8、风险排查,安全加固	9
9、加固	

# 目 录

# 一、自査

# Linux 系统

#### 1、Pwnrig 挖矿

在 root 权限命令行执行: find / -name \*pwnrig\* 如果有文件显示,那么就属于中了 pwnrig 挖矿 删除 pwnrig 文件 find / -name \*pwnrig\* | xargs rm -rf 检查服务 chkconfig -list 删除 pwnrig 有关服务 chkconfig -del "pwnrig 服务名" 更改弱口令密码,设置强密码(大于 8 位),设置登录策略,设置 ssh 秘钥登录, 进行服务器整改安全加固

# 2、PhoenixMiner 挖矿

在 root 权限命令行执行: find / -name .x 注意这是个隐藏目录。 1s -a1 查看隐藏文件 进入目录之后,文件如下所示,存在 start\_miner.sh 那么就属于 PhoenixMiner 挖矿

大小	压缩后大小	类型	修改时间	CRC32
		文件夹		
		文件夹	2022/4/1 9:04	
182	164	.file	2020/12/28 21:25	3AC0735B
51,051	7,421	文本文档	2021/10/30 10:57	6A10438E
61,540,757	7,524,523	文本文档	2021/11/1 15:54	585CF80F
9,328,412	4,878,605	.file	2020/11/27 3:24	9B5D7F23
976	341	.file	2020/12/5 2:06	6AAAF4
290	235	SH 文件	2020/12/28 21:25	11297BB5
	大小 182 51,051 61,540,757 9,328,412 976 290	大小 压缩后大小   182 164   51,051 7,421   61,540,757 7,524,523   9,328,412 4,878,605   976 341   290 235	大小 压缩后大小 美型   文件実 文件実   182 164 file   51,051 7,421 文本文档   61,540,757 7,524,523 文本文档   9,328,412 4,878,605 file   976 341 file   290 235 SH 文件	大小压缩后大小类型修改时间マ件夹文件夹文件支2022/4/19:04182164file2020/12/28 21:2551,0517,421文本文档2021/10/30 10:5761,540,7577,524,523文本文档2021/11/11 15:549,328,4124,878,605file2020/11/27 3:24976341file2020/12/5 2:06290235SH 文件2020/12/28 21:25

删除.x目录 rm -rf ./.x 更改弱口令密码,设置强密码(大于8位),设置登录策略,设置 ssh 秘钥登录, 进行服务器整改安全加固

## 3、.font-unix 挖矿

在 root 权限命令行执行: find / -name .font-unix 注意这是个隐藏目录。 1s -a1 查看隐藏文件 进入目录之后,文件如下所示,那么就属于.font-unix 挖矿

名称    ^	大小	压缩后大小 类型	修改时间	CRC32
II.		文件夹		
admin	355	? .file	2019/8/9 14:58	
config.txt	0	? 文本文档	2021/8/1 7:47	
🗋 cron.d	54	? D 文件	2022/3/12 22:12	
doos.pid	5	? PID 文件	2022/3/23 10:25	
epools.txt	105	? 文本文档	2022/3/12 22:12	
	16,371,712	? .file	2022/3/30 19:46	
l.old	227,658,986	? OLD 文件	2022/3/23 10:12	
🗋 mysql	838,583	? .file	2016/2/21 0:58	
📄 nano.backup	185	? BACKUP 文件	2022/3/12 22:12	
new.dir	16	? DIR 文件	2022/3/12 22:12	
python	9,590,140	? .file	2021/11/2 3:55	
root.sh	276	? SH 文件	2021/1/13 15:49	

删除删除.font-unix 目录 rm -rf ./.font-unix 更改弱口令密码,设置强密码(大于 8 位),设置登录策略,设置 ssh 秘钥登录, 进行服务器整改安全加固

# 4、伪装 python 程序挖矿

在 root 权限命令行执行: find / -name .opt 注意这是个隐藏目录。 1s -a1 查看隐藏文件 进入目录之后,文件如下所示,那么就属于伪 python 挖矿

× ×	1140	X.J.	113110月八小	X III	Sherren aleg	CIUSE
1 6,529,328 6,529,328 ,file 2022/3/111528 3691E535   2 147 146 ,file 2022/3/111528 65819D   a 241 181 ,file 2022/3/111528 65819D   bashpid 5 5 PID.XIF 20022/3/111528 383076F4   c 2,318 466 ,file 2022/3/111528 333076F4   c conda.psm1 9,049 2,805 Windows PowerS 2022/3/111528 3130CF68   conda.psm1 9,049 2,805 Windows PowerS 2022/3/111528 66990767   conda.psm1 9,049 2,805 Windows PowerS 2022/3/111625 69984377   conda.psm1 11 146 Python File 2022/3/111528 60970767   conda 78 58 D X/# 2022/3/111528 60970767   dir.dir 10 10 D10 X2 2022/3/111528 65809204   h 838,583 297,947 file 2022/3/111528 65805	J			文件夹		
2 147 146. file 2022/y111528 65819D.   b a 241 181. file 2022/y111528 65819D.   bahpid 5 5 PID 文件 2022/y111528 33876FE4   c 2,318 468. file 2022/y111528 AF4FEB66   conda.psm1 9,049 2,805 Windows PowerS. 2022/y111625 G69B4377   conda.psm1 9,049 2,805 Windows PowerS. 2022/y111625 G69B4377   conda.psm1 9,049 2,805 Windows PowerS. 2022/y111625 G69B4377   conda.psm1 0 10 D,018 文件 2022/y111528 G6995084   conda.psm3 10 0 D,018 文件 2022/y111528 G6995084   idrafi 10 D,018 文件 2022/y111528 G695084 G695084   hide 838,583 297,949 file 2022/y111528 G695084   proxy 17 17. file 2022/y111528 G5819294   nona 6,530,329 file 2022/y111528 <td>]1</td> <td>6,529,328</td> <td>6,529,328</td> <td>.file</td> <td>2022/3/11 15:28</td> <td>3691E535</td>	]1	6,529,328	6,529,328	.file	2022/3/11 15:28	3691E535
a 241 181. file 2022/3/11 1528 E9CASCC2   bah.pid 5 5 PID X# 2022/3/11 1528 38876FE4   c 2,318 468. file 2022/3/11 1528 38876FE4   c conda.hook.ps1 9,049 2,805 Windows PowerS. 2022/3/11 1625 31380EBE   conda.hook.ps1 344 192 Windows PowerS. 2022/3/11 1625 6691BEBI   condia.psm 134 192 Windows PowerS. 2022/3/11 1528 66991BEBI   condia.psm 161 146 Python File 2022/3/11 1528 669970FB   conda.hook.ps1 01 10 DIR X# 2022/3/11 1528 669970FB   idridir 10 10 DIR X# 2022/3/11 1528 86950B4   hide 838,583 297,949 file 2022/3/11 1528 E786752   prixon 17 17. file 2022/3/11 1528 E786752 2980752   putn 36 6,530.329 6,530.329. file 2022/3/11 1528 E786752 <t< td=""><td>2</td><td>147</td><td>146</td><td>.file</td><td>2022/3/11 15:28</td><td>65819D</td></t<>	2	147	146	.file	2022/3/11 15:28	65819D
bash.pid 5 5 PID.文件 2022/y111528 33876F4F   c 2,318 468.file 2022/y111528 A4FEF868   c 0nda.psm1 9,049 2,805 Windows PowerS 2022/y111625 G691827   c 0ndia.psm1 9,049 2,805 Windows PowerS 2022/y111625 G6918437   c 0ndia.psm1 144 192 Windows PowerS 2022/y111625 G6918437   c ondia.psm1 146 Python File 2022/y111528 60970976   dir.dir 10 D IR 文件 2022/y111528 60970976   dir.dir 10 D IR 文件 2022/y111528 60970976   ndrad 838,583 297,949 file 2022/y111528 60950964   ndrad 839,584 297,937 file 2022/y111528 66950964   ndrad 839,584 297,937 file 2022/y111528 6596024   proxy 17 17 file 2022/y111528 5506023 6,	a	241	181	.file	2022/3/11 15:28	E9CA5CCE
c 2,318 468. file 2022/3/111528 A4FEFB68   Conda, book,ps1 9,049 2,805 Windows PowerS 2022/3/111625 C6918E81   conda, hook,ps1 344 192 Windows PowerS 2022/3/111625 C6918E81   conda, hook,ps1 344 192 Windows PowerS 2022/3/111625 C6918E81   conda, fig.py 151 146 Python File 2022/3/111528 C691970F5   dir,dir 10 10 DIR, %# 2022/3/111528 C691970F5   dir,dir 10 10 DIR, %# 2022/3/111528 C691920F3   hade 839,584 297.997 file 2022/3/111528 C69120F3   proxy 17 17 file 2022/3/111528 C69120F3   python36 6,530,329 6,530,329 file 2022/3/111528 C5018023   upd 220 197 file 2022/3/111284 C5018023   upd 220 197 file 2022/3/111284 C5018023	bash.pid	5	5	PID 文件	2022/3/11 15:28	33B76FE4
Orndapsm1 9,049 2,805 Windows PowerS 2022/3/111625 3138/058   conda-hookps1 344 192 Windows PowerS 2022/3/111625 C6918/E81   conday 151 146 Python File 2022/3/111625 C6918/E81   cronda 78 58 D X/# 2022/3/111528 C6970761   dirdidr 10 10 DIR X/# 2022/3/111528 C6970761   proxy 17 10 ID R X/# 2022/3/111528 E692084   nide 839,584 297937 co22/3/111528 E692084   nide 839,584 297937 co22/3/111528 E692084   nide 839,584 297937 co22/3/111528 E780C752   proxy 17 17 file 2022/3/111528 E780C752   python36 6,530,329 file 2022/3/111528 E502802   upd 220 177 file 2022/3/111528 E4FCE17F   user 10 10 file	] c	2,318	468	.file	2022/3/11 15:28	A4FEFB68
aconda-hook.ps1 344 192 Windows PowerS. 2022/3/11 CC 69118EB1   config.py 151 146 Python File 2022/3/11 6520 65984377   fordid 78 SB D.Xft 2022/3/11 1528 76485799   firdidr 10 DIR.Xft 2022/3/11 586 5970475   firdidr 10 DIR.Xft 2022/3/11 586 595044   hide 839,584 297.997 file 2022/3/11 586 595044   hide 839,584 297.997 file 2022/3/11 586 595044   proxy 17 17 file 2022/3/11 586 575.672   python36 6,530,329 6,530,329 file 2022/3/11 586 5501602   upd 220 197.file 2022/3/11 286 5501602   upd 220 197.file 2022/3/11 286 55016102   upd 220 107 file 2022/3/11	a Conda.psm1	9,049	2,805	Windows PowerS	2022/3/11 16:25	3138CBF8
config.py 151 146 Python File 2022/3/11 66 6984377   crond 78 58 D X/H 2022/3/11 58 67970F5   idr.dir 10 10 D IR X/H 2022/3/11 58 67486799   h 838,583 297,949 file 2022/3/11 58 66969377   prix 839,584 297,937 file 2022/3/11 58 66969204   hide 839,584 297,937 file 2022/3/11 58 68695204   proxy 17 17 file 2022/3/11 58 6286752   prino36 6,530,329 6,530,329 file 2022/3/11 58 6508023   un 896 375 file 2022/3/11 58 65018023   upd 220 197 file 2022/3/11 58 65018023   upd 220 197 file 2022/3/11 58 F35EEFC   user 10 <	🗟 conda-hook.ps1	344	192	Windows PowerS	2022/3/11 16:25	C691BEB1
orond 78 58 D X/# 2022/3/11 15:28 60970765   dir.dir 10 10 D IR X/# 2022/3/11 15:28 60970765   h 838,563 297,949 .16 2022/3/11 15:28 6695064   inde 839,564 297,937 .16 2022/3/11 15:28 6695064   proxy 17 17 .16 2022/3/11 15:28 C5286275   python36 6,530,329 .6,530,329 .16 2022/3/11 15:28 C5DE0023   upd 2020 197 .16 2022/3/11 15:28 C5DE0023   upd 220 197 .16 2022/3/11 15:28 C5DE0023   user 10 10 .16 2022/3/11 12:28 F735EETC   user 24 24 24 2022/3/11 15:28 F735EETC	🗟 config.py	151	146	Python File	2022/3/11 16:50	6E9B4377
dir.dir 10 10 DIR 文件 2022/3/11 528 7E482799   h 838,583 297,949 file 2022/3/11 528 8695004   hide 839,584 297,937 file 2022/3/11 528 8695004   proxy 17 17 file 2022/3/11 528 2F38C752   python36 6,530,329 6,530,329 file 2022/3/11 528 2F38C752   upd 202 197 file 2022/3/11 1528 CSDB023   upd 220 197 file 2022/3/11 1528 E4F25E7   user 10 10 file 2022/3/11 1528 FF35EE7C   user 24 24 4.file 2022/3/11 1528 FF35EE7C	cron.d	78	58	D文件	2022/3/11 15:28	6D9770F5
h 838,583 297,949 file 2022/3/11528 68695094   hide 839,584 297,937 file 2022/3/111528 506FE501E   proxy 17 17 file 2022/3/111528 2F38C752   python36 6,530,329 6,530,329 file 2022/3/111528 2F38C752   un 896 375 file 2022/3/111528 CSDE8023   upd 220 197 file 2022/3/111528 CSDE8023   upd 220 197 file 2022/3/111528 F35EEFC   user 10 10 file 2022/3/111528 F535EEFC   x 224 24 24 202/3/111528 F535EEFC	] dir.dir	10	10	DIR 文件	2022/3/11 15:28	7E48E799
Inde 839,584 297,937 file 2022/y111528 CEFESTS   prixexy 17 17.16 2022/y111528 ZEBGC52   python36 6,530,329 6,530,329 file 2022/y111528 ZEBGC52   unn 896 375 file 2022/y111528 CSDB0022   upd 220 197 file 2022/y1112048 EAFCE17F   user 10 10.16 2022/y111528 FF35EEFC   x 24 24 24 2022/y111528 FF35EEFC	h	838,583	297,949	.file	2022/3/11 15:28	869E9DB4
proxy 17 17. file 2022/3/11 15:28 2F38C752   python36 6,530,329 6,530,329 file 2022/3/11 15:28 2F38C752   unn 896 375. file 2022/3/11 15:28 CSDB023   upd 220 197. file 2022/3/11 15:28 CSDB023   upd 220 197. file 2022/3/11 15:28 FF35EEFC   user 10 10. file 2022/3/11 15:28 FF35EEFC   x 24 24 4.file 2022/3/11 15:28 FF35EEFC	hide	839,584	297,937	.file	2022/3/11 16:35	CBEFE51E
python36 6,530,329 6,530,329 file 2022/y111549 A S16EFER   run 896 375 file 2022/y111528 C5DE8023   upd 220 197 file 2022/y111248 E4FCE177   user 10 10 file 2022/y111528 F735EEFC   x 24 24 24 2022/y111528 F355EFC	proxy	17	17	.file	2022/3/11 15:28	2F38C752
run 896 375 file 2022/3/11 52.8 CSDE8023   upd 220 197 file 2022/3/11 52.04 E4FCE177   user 10 10 file 2022/3/11 52.08 FF35EEFC   x 24 24 file 2022/3/11 52.08 F935EEFC	python36	6,530,329	6,530,329	.file	2022/3/11 15:49	A516EFEB
upd 220 197 file 2022/3/11 20.48 E4FCE17F   user 10 10 file 2022/3/11 52.88 F35EEFC   x 24 24 24 24 2022/3/11 52.98 5301A119	] run	896	375	.file	2022/3/11 15:28	C5DEB023
user 10 10 .file 2022/3/11 15:28 FF35EEFC x 24 24 .file 2022/3/11 15:28 5901A119	upd	220	197	.file	2022/3/11 20:48	E4FCE17F
x 24 24 file 2022/3/11 15:28 5901A119	Juser	10	10	.file	2022/3/11 15:28	FF35EEFC
	x	24	24	.file	2022/3/11 15:28	5901A119

删除删除.opt 目录 rm -rf ./.opt 更改弱口令密码,设置强密码(大于 8 位),设置登录策略,设置 ssh 秘钥登录, 进行服务器整改安全加固

# webminer 挖矿

检查以下目录是否存在对应的 js 文件 名字类似的即可	
删除文件	
%HOMEPATH%\AppData\Local\Microsoft\Windows\Temporary	Internet
Files\Content.IE5\I79ELXX6\wp-emoji-release.min[1].js	
%HOMEPATH%\AppData\Local\Microsoft\Windows\Temporary	Internet
Files\Content.IE5\LG9KLAT2\site[1].js	
%HOMEPATH%\AppData\Local\Microsoft\Windows\Temporary	Internet
Files\Content.IE5\LG9KLAT2\responsive-nav[1].js	
%HOMEPATH%\AppData\Local\Microsoft\Windows\Temporary	Internet
Files\Content.IE5\I79ELXX6\stickUp[1].js	
%HOMEPATH%\AppData\Local\Microsoft\Windows\Temporary	Internet
Files\Content.IE5\23RZZJCQ\wp-embed.min[1].js	
%HOMEPATH%\AppData\Local\Microsoft\Windows\Temporary	Internet
Files\Content.IE5\I79ELXX6\coinhive.min[1].js	
或者使用 everything 软件进行检索"coinhive"、"xmrig"等关键字	
检索到之后删除目标文件之后,利用腾讯杀毒软件进行全盘杀毒	

用杀毒软件进行全盘杀毒,看是否存在挖矿程序,若有则清理挖矿等木马程序,若无则进行以下安全加固

# 1、安装杀毒软件修复系统漏洞和打补丁

- 1、安装安全软件并升级病毒库,定期全盘扫描,保持实时防护
- 2、及时更新 Windows 安全补丁,开启防火墙临时关闭端口
- 3、及时更新 web 漏洞补丁,升级 web 组件

# 2、关闭高危漏洞

新的挖矿攻击展现出了类似蠕虫的行为,并结合了高级攻击技术,以增加对目标服务器感染的成功率。通过利用永恒之蓝(EternalBlue)、web 攻击多种漏洞,如 Tomcat 弱口令攻击、Weblogic WLS 组件漏洞、Jboss 反序列化漏洞,Struts2 远程命令执行等,导致大量服务器被感染挖矿程序的现象。总结了几种预防措施:

1) 安装安全软件并升级病毒库,定期全盘扫描,保持实时防护

2) 及时更新 Windows 安全补丁,开启防火墙临时关闭端口 445,139 等永恒之蓝的高危端口可以关闭。

## 3、修复第三方软件漏洞

如果您服务器内有运行对外应用软件(WWW、FTP 等),请您对软件进行配置,限制应用程序的权限,禁止目录浏览或文件写权限。

开启 Web 应用防火墙 防护, 查看 Web 应用防护攻击日志。

Tomcat、Weblogic WLS 组件、Jboss, Struts2 等中间件和 web 组件等检查对应的漏洞是否已经修复,检查更新到最新版本。

# 二、常用处理

## 1、及时隔离主机

部分带有蠕虫功能的挖矿木马在取得主机的控制权后,会继续对公网的其他主机, 或者以当前主机作为跳板机对同一局域网内的其他主机进行横向渗透,所以在发 现主机被植入挖矿木马后,在不影响业务正常运行的前提下,应该及时隔离受感 染的主机,然后进行下一步分析和清除工作。

#### 2、阻断异常网络通信

挖矿木马不仅会连接矿池,还有可能会连接黑客的 C2 服务器,接收并执行 C2 指 令、投递其他恶意木马,所以需要及时进行网络阻断。 检查主机防火墙当前生效的 iptables 规则中是否存在业务范围之外的可疑地址 和端口,它们可能是挖矿木马的矿池或 C2 地址 iptables -L - n

从 iptables 规则中清除可疑地址和端口

vi /etc/sysconfig/iptables

阻断挖矿木马的网络通信

iptables -A INPUT -s 可疑地址 -j DROPiptables -A OUTPUT -d 可疑地址 -j DROP

# 3、清除定时任务

查看系统当前用户的计划任务: crontab -1 查看系统特定用户的计划任务: crontab -u username -1 查看其他计划任务文件: cat /etc/crontab cat /var/spool/cron cat /etc/cron.d/ cat /etc/cron.daily/ cat /etc/cron.hourly/ cat /etc/cron.weekly/ cat /etc/cron.monthly/ cat /var/spool/cron/

# 4、清除启动项

除了计划任务,挖矿木马通过添加启动项同样能实现持久化。可以使用如下命 令查看开机启动项中是否有异常的启动服务。

CentOS7 以下版本:

chkconfig -list

CentOS7 及以上版本:

systemctl list-unit-files

如果发现有恶意启动项,可以通过如下命令进行关闭:

CentOS7 以下版本:

chkconfig 服务名 off

CentOS7 及以上版本:

systemctl disable 服务名

还需要仔细排查以下目录及文件,及时删除可疑的启动项: /usr/lib/systemd/system /usr/lib/systemd/system/multi-user.target.wants /etc/rc.local /etc/rc0.d/ /etc/rc0.d/ /etc/rc2.d/ /etc/rc3.d/ /etc/rc5.d/ /etc/rc6.d/ /etc/rc6.d/

## 5、清除预加载 so

通过配置/etc/ld.so.preload,可以自定义程序运行前优先加载的动态链接库, 部分木马通过修改该文件,添加恶意 so 文件,从而实现挖矿进程的隐藏等恶意 功能。

检查/etc/ld.so.preload(该文件默认为空),清除异常的动态链接库

# 6、清除 ssh 公钥

挖矿木马通常还会在<sup>~</sup>/.ssh/authoruzed\_keys 文件中写入黑客的 SSH 公钥,这 样子就算用户将挖矿木马清除得一干二净,黑客还是可以免密登陆该主机,这也 是常见的保持服务器控制权的手段。

排查<sup>~</sup>/.ssh/authorized\_keys 文件,如果发现可疑的 SSH 公钥,直接删除。

# 7、清除挖矿木马

(1) 清除挖矿进程

挖矿木马最大的特点就是会在用户不知情的情况下,利用主机的算力进行挖矿, 从而消耗主机大量的 CPU 资源,所以,通过执行如下命令排查系统中占用大量 CPU 资源的进程 挖矿木马最大的特点就是会在用户不知情的情况下,利用主机的算力进行挖 矿,从而消耗主机大量的 CPU 资源,所以,通过执行如下命令排查系统中占用 大量 CPU 资源的进程。

#### top -cps -ef

确认相关进程为挖矿进程后,按照如下步骤将其清除: 获取并记录挖矿进程的 文件路径:

ls -l /proc/**\$PID**/exe

杀死挖矿进程:

kill -9 \$PID

删除挖矿进程对应的文件

#### 8、风险排查,安全加固

1. 木马复辟

主要因为清除得不够彻底。大部分用户都只是 Kill 掉挖矿进程和对应文件,却没有清理计划任务和守护进程。

一般建议先清除计划任务、启动项、守护进程,再清除挖矿进程和其他恶意进程。

2. 判定恶意进程

假如未知进程 kinsing 监听本地 31458 端口,非常可疑,可通过如下方法判定: (1)执行`1s -a1 /proc/\$PID/exe`确认可疑进程对应的文件;

(2)若文件未被删除,则直接上传文件到 Virustotal 进行检测,或者计算出文件对应的 md5,使用 md5 去 Virustotal 进行查询;若文件已被删除,可执行`cat /proc/\$PID/exe > /tmp/t.bin`将进程 dump 到特定目录,再上传文件到 Virustotal 或者计算 dump 文件对应的 md5 到 Virustotal 进行查询。如果有多款杀毒引擎同时检出,那基本可以判定该进程为恶意进程。

系统 CPU 占用率接近 100%, 却看不到是哪个进程导致的, 这种情况一般是因为 系统命令被木马篡改了, 从而隐藏了木马进程的踪迹, 让用户无法进行溯源分析。 可尝试如下方案解决: 安装 busybox 来对系统进行排查。

busybox 是一个集成了 300 多个最常用 Linux 命令和工具的软件,可以使用 busybox 替代系统命令对系统进行排查;

yum -y install wget make gcc perl glibc-static ncurses-devel libgcryptdevel

wget http://busybox.net/downloads/busybox-1.33.0.tar.bz2tar -jxvf busybox-1.33.0.tar.bz2

cd busybox-1.33.0 && make && make install

# 9、加固

(一)、检查隐藏帐户及弱口令

检查服务器系统及应用帐户是否存在 弱口令:

检查说明:检查管理员帐户、数据库帐户、MySQL 帐户、tomcat 帐户、网站后 台管理员帐户等密码设置是否较为简单,简单的密码很容易被黑客破解。 解决方法:以管理员权限登录系统或应用程序后台,修改为复杂的密码。

(二)、检查第三方软件漏洞(中间件等)

1、如果您服务器内有运行 Web、数据库等应用服务,请您限制应用程序帐户对 文件系统的写权限,同时尽量使用非 root 帐户运行。

检查说明:使用非 root 帐户运行,可以保障在应用程序被攻陷后,攻击者无法 立即远程控制服务器,减少攻击损失。

解决方法:

进入 web 服务根目录或数据库配置目录。

运行 chown -R apache:apache /var/www/xxxx、chmod -R 750 file1.txt 命令 配置网站访问权限。

2、升级修复应用程序漏洞

检查说明:机器被入侵,部分原因是系统使用的应用程序软件版本较老,存在较多的漏洞而没有修复,导致可以被入侵利用。

解决方法:比较典型的漏洞例如 ImageMagick、openss1、glibc 等,用户可以 根据腾讯云已发布的安全通告指导或通过 apt-get/yum 等方式进行直接升级修 复。

#### 网站目录文件权限的参考示例如下:

场景:

假设 HTTP 服务器运行的用户和用户组是 www,网站用户为 centos,网站根目录是 /home/centos/web。

方法/步骤:

1. 我们首先设定网站目录和文件的所有者和所有组为 centos, www, 如下命令:

chown -R centos:www /home/centos/web

 设置网站目录权限为750,750是 centos 用户对目录拥有读写执行的权限,设置后, centos 用户可以在任何目录下创建文件,用户组有有读执行权限,这样才能进入目录,其 它用户没有任何权限。

find -type d -exec chmod 750 {} \;

3. 设置网站文件权限为 640, 640 指只有 centos 用户对网站文件有更改的权限, HTTP 服 务器只有读取文件的权限,无法更改文件,其它用户无任何权限。

find -not -type d -exec chmod 640 {} \;

4. 针对个别目录设置可写权限。例如,网站的一些缓存目录就需要给 HTTP 服务有写入权限、discuz x2 的/data/目录就必须要写入权限。

find data -type d -exec chmod 770 {} \;

# 被入侵后的安全优化建议

推荐使用 SSH 密钥进行登录,减少暴力破解的风险。

在服务器内编辑/etc/ssh/sshd\_config 文件中的 Port 22, 将 22 修改为其他非默 认端口,修改之后重启 SSH 服务。可使用如下命令重启:

/etc/init.d/sshd restart(CentOS)或 /etc/init.d/ssh restart (Debian/Ubuntu)

如果必须使用 SSH 密码进行管理,选择一个好密码。

无论应用程序管理后台(网站、中间件、tomcat 等)、远程 SSH、远程桌面、数据库, 都建议设置复杂且不一样的密码。

下面是一些好密码的实例(可以使用空格):

1qtwo-threeMiles3c45jia

caser, lanqiu streets

下面是一些弱口令的示例,可能是您在公开的工作中常用的词或者是您生活中常用的词:

公司名+日期(coca-cola2016xxxx)

常用口语(Iamagoodboy)

使用以下命令检查主机有哪些端口开放,关闭非业务端口。

#### netstat -antp

应用程序尽量不使用 root 权限。

例如 Apache、Redis、MySQL、Nginx 等程序,尽量不要以 root 权限的方式运行。 修复系统提权漏洞与运行在 root 权限下的**程序漏洞**,以免恶意软件通过漏洞提权获得 root 权限传播后门。

及时更新系统或所用应用程序的版本,如 Struts2、Nginx, ImageMagick、Java 等。 关闭应用程序的远程管理功能,如 Redis、NTP 等,如果无远程管理需要,可关闭对外 监听端口或配置。

定期备份云服务器业务数据。

对重要的业务数据进行异地备份或云备份,避免主机被入侵后无法恢复。 除了您的 home, root 目录外,您还应当备份 /etc 和可用于取证的 /var/log 目录。