专注APT攻击与防御
https://micropoor.blogspot.com/

**exp注：**

CVE-2017-1000367 [Sudo]
(Sudo 1.8.6p7 - 1.8.20)

CVE-2017-1000112 [a memory corruption due to UFO to non-UFO path switch]

CVE-2017-7494 [Samba Remote execution]
(Samba 3.5.0-4.6.4/4.5.10/4.4.14)

CVE-2017-7308 [a signedness issue in AF_PACKET sockets]
(Linux kernel through 4.10.6)

CVE-2017-6074 [a double-free in DCCP protocol]
(Linux kernel through 4.9.11)

CVE-2017-5123 ['waitid()']
(Kernel 4.14.0-rc4+)

CVE-2016-9793 [a signedness issue with SO_SNDBUFFORCE and SO_RCVBUFFORCE socket options]
(Linux kernel before 4.8.14)

CVE-2016-5195 [Dirty cow]
(Linux kernel>2.6.22 (released in 2007))

CVE-2016-2384 [a double-free in USB MIDI driver]
(Linux kernel before 4.5)

CVE-2016-0728 [pp_key]
(3.8.0, 3.8.1, 3.8.2, 3.8.3, 3.8.4, 3.8.5, 3.8.6, 3.8.7, 3.8.8, 3.8.9, 3.9, 3.10, 3.11, 3.12, 3.13, 3.4.0, 3.5.0, 3.6.0, 3.7.0, 3.8.0, 3.8.5, 3.8.6, 3.8.9, 3.9.0, 3.9.6, 3.10.0, 3.10.6, 3.11.0,

3.12.0, 3.13.0, 3.13.1)

CVE-2015-7547 [glibc getaddrinfo]
(before Glibc 2.9)

CVE-2015-1328 [overlayfs]
(3.13, 3.16.0, 3.19.0)

CVE-2014-5284 [OSSEC]
(2.8)

CVE-2014-4699 [ptrace]
(before 3.15.4)

CVE-2014-4014 [Local Privilege Escalation]
(before 3.14.8)

CVE-2014-3153 [futex]
(3.3.5 ,3.3.4 ,3.3.2 ,3.2.13 ,3.2.9 ,3.2.1 ,3.1.8 ,3.0.5 ,3.0.4 ,3.0.2 ,3.0.1 ,2.6.39 ,2.6.38 ,2.6.37 ,2.6.35 ,2.6.34 ,2.6.33 ,2.6.32 ,2.6.9 ,2.6.8 ,2.6.7 ,2.6.6 ,2.6.5 ,2.6.4 ,3.2.2 ,3.0.18 ,3.0 ,2.6.8.1)

CVE-2014-0196 [rawmodePTY]
(2.6.31, 2.6.32, 2.6.33, 2.6.34, 2.6.35, 2.6.36, 2.6.37, 2.6.38, 2.6.39, 3.14, 3.15)

CVE-2014-0038 [timeoutpwn]
(3.4, 3.5, 3.6, 3.7, 3.8, 3.8.9, 3.9, 3.10, 3.11, 3.12, 3.13, 3.4.0, 3.5.0, 3.6.0, 3.7.0, 3.8.0, 3.8.5, 3.8.6, 3.8.9, 3.9.0, 3.9.6, 3.10.0, 3.10.6, 3.11.0, 3.12.0, 3.13.0, 3.13.1)

CVE-2013-2094 [perf_swevent]
(3.0.0, 3.0.1, 3.0.2, 3.0.3, 3.0.4, 3.0.5, 3.0.6, 3.1.0, 3.2, 3.3, 3.4.0, 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.4.6, 3.4.8, 3.4.9, 3.5, 3.6, 3.7, 3.8.0, 3.8.1, 3.8.2, 3.8.3, 3.8.4, 3.8.5, 3.8.6, 3.8.7, 3.8.8, 3.8.9)

CVE-2013-1858 [clown-newuser]

(3.3-3.8)

CVE-2013-1763 [__sock_diag_rcv_msg]
(before 3.8.3)

CVE-2013-0268 [msr]
(2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.25, 2.6.26, 2.6.27, 2.6.27, 2.6.28, 2.6.29, 2.6.30, 2.6.31, 2.6.32, 2.6.33, 2.6.34, 2.6.35, 2.6.36, 2.6.37, 2.6.38, 2.6.39, 3.0.0, 3.0.1, 3.0.2, 3.0.3, 3.0.4, 3.0.5, 3.0.6, 3.1.0, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7.0, 3.7.6)

CVE-2012-3524 [libdbus]
(libdbus 1.5.x and earlier)

CVE-2012-0056 [memodipper]
(2.6.39, 3.0.0, 3.0.1, 3.0.2, 3.0.3, 3.0.4, 3.0.5, 3.0.6, 3.1.0)

CVE-2010-4347 [american-sign-language]
( 2.6.0, 2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 2.6.6, 2.6.7, 2.6.8, 2.6.9, 2.6.10, 2.6.11, 2.6.12, 2.6.13, 2.6.14, 2.6.15, 2.6.16, 2.6.17, 2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30, 2.6.31, 2.6.32, 2.6.33, 2.6.34, 2.6.35, 2.6.36)

CVE-2010-4258 [full-nelson]
(2.6.31, 2.6.32, 2.6.35, 2.6.37)

CVE-2010-4073 [half_nelson]
(2.6.0, 2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 2.6.6, 2.6.7, 2.6.8, 2.6.9, 2.6.10, 2.6.11, 2.6.12, 2.6.13, 2.6.14, 2.6.15, 2.6.16, 2.6.17, 2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30, 2.6.31, 2.6.32, 2.6.33, 2.6.34, 2.6.35, 2.6.36)

CVE-2010-3904 [rds]
(2.6.30, 2.6.31, 2.6.32, 2.6.33, 2.6.34, 2.6.35, 2.6.36)

CVE-2010-3437 [pktcdvd]
(2.6.0, 2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 2.6.6, 2.6.7, 2.6.8, 2.6.9, 2.6.10, 2.6.11, 2.6.12, 2.6.13, 2.6.14, 2.6.15, 2.6.16, 2.6.17, 2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24,

2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30, 2.6.31, 2.6.32, 2.6.33, 2.6.34, 2.6.35, 2.6.36)

CVE-2010-3301 [ptrace_kmod2]
(2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30, 2.6.31, 2.6.32, 2.6.33, 2.6.34)

CVE-2010-3081 [video4linux]
(2.6.0, 2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 2.6.6, 2.6.7, 2.6.8, 2.6.9, 2.6.10, 2.6.11, 2.6.12, 2.6.13, 2.6.14, 2.6.15, 2.6.16, 2.6.17, 2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30, 2.6.31, 2.6.32, 2.6.33)

CVE-2010-2959 [can_bcm]
(2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30, 2.6.31, 2.6.32, 2.6.33, 2.6.34, 2.6.35, 2.6.36)

CVE-2010-1146 [reiserfs]
(2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30, 2.6.31, 2.6.32, 2.6.33, 2.6.34)

CVE-2010-0415 [do_pages_move]
(2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30, 2.6.31)

CVE-2009-3547 [pipe.c_32bit]
(2.4.4, 2.4.5, 2.4.6, 2.4.7, 2.4.8, 2.4.9, 2.4.10, 2.4.11, 2.4.12, 2.4.13, 2.4.14, 2.4.15, 2.4.16, 2.4.17, 2.4.18, 2.4.19, 2.4.20, 2.4.21, 2.4.22, 2.4.23, 2.4.24, 2.4.25, 2.4.26, 2.4.27, 2.4.28, 2.4.29, 2.4.30, 2.4.31, 2.4.32, 2.4.33, 2.4.34, 2.4.35, 2.4.36, 2.4.37, 2.6.15, 2.6.16, 2.6.17, 2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30, 2.6.31)

CVE-2009-2698 [udp_sendmsg_32bit]
(2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 2.6.6, 2.6.7, 2.6.8, 2.6.9, 2.6.10, 2.6.11, 2.6.12, 2.6.13, 2.6.14, 2.6.15, 2.6.16, 2.6.17, 2.6.18, 2.6.19)

CVE-2009-2692 [sock_sendpage]

(2.4.4, 2.4.5, 2.4.6, 2.4.7, 2.4.8, 2.4.9, 2.4.10, 2.4.11, 2.4.12, 2.4.13, 2.4.14, 2.4.15, 2.4.16, 2.4.17, 2.4.18, 2.4.19, 2.4.20, 2.4.21, 2.4.22, 2.4.23, 2.4.24, 2.4.25, 2.4.26, 2.4.27, 2.4.28, 2.4.29, 2.4.30, 2.4.31, 2.4.32, 2.4.33, 2.4.34, 2.4.35, 2.4.36, 2.4.37, 2.6.0, 2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 2.6.6, 2.6.7, 2.6.8, 2.6.9, 2.6.10, 2.6.11, 2.6.12, 2.6.13, 2.6.14, 2.6.15, 2.6.16, 2.6.17, 2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30)

CVE-2009-2692 [sock_sendpage2]
(2.4.4, 2.4.5, 2.4.6, 2.4.7, 2.4.8, 2.4.9, 2.4.10, 2.4.11, 2.4.12, 2.4.13, 2.4.14, 2.4.15, 2.4.16, 2.4.17, 2.4.18, 2.4.19, 2.4.20, 2.4.21, 2.4.22, 2.4.23, 2.4.24, 2.4.25, 2.4.26, 2.4.27, 2.4.28, 2.4.29, 2.4.30, 2.4.31, 2.4.32, 2.4.33, 2.4.34, 2.4.35, 2.4.36, 2.4.37, 2.6.0, 2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 2.6.6, 2.6.7, 2.6.8, 2.6.9, 2.6.10, 2.6.11, 2.6.12, 2.6.13, 2.6.14, 2.6.15, 2.6.16, 2.6.17, 2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29, 2.6.30)

CVE-2009-1337 [exit_notify]
(2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29)

CVE-2009-1185 [udev]
(2.6.25, 2.6.26, 2.6.27, 2.6.28, 2.6.29)

CVE-2008-4210 [ftrex]
(2.6.11, 2.6.12, 2.6.13, 2.6.14, 2.6.15, 2.6.16, 2.6.17, 2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22)

CVE-2008-0600 [vmsplice2]
(2.6.23, 2.6.24)

CVE-2008-0600 [vmsplice1]
(2.6.17, 2.6.18, 2.6.19, 2.6.20, 2.6.21, 2.6.22, 2.6.23, 2.6.24, 2.6.24.1)

CVE-2006-3626 [h00lyshit]
(2.6.8, 2.6.10, 2.6.11, 2.6.12, 2.6.13, 2.6.14, 2.6.15, 2.6.16)

CVE-2006-2451 [raptor_prctl]
(2.6.13, 2.6.14, 2.6.15, 2.6.16, 2.6.17)

CVE-2005-0736 [krad3]
(2.6.5, 2.6.7, 2.6.8, 2.6.9, 2.6.10, 2.6.11)

CVE-2005-1263 [binfmt_elf.c]
(Linux kernel 2.x.x to 2.2.27-rc2, 2.4.x to 2.4.31-pre1, and 2.6.x to 2.6.12-rc4)

CVE-2004-1235 [elflbl]
(2.4.29)

CVE-N/A [caps_to_root]
(2.6.34, 2.6.35, 2.6.36)

CVE-2004-0077 [mremap_pte]
(2.4.20, 2.2.24, 2.4.25, 2.4.26, 2.4.27)

**已对外公开exp注：**

https://github.com/SecWiki/linux-kernel-exploits
https://github.com/Kabot/Unix-Privilege-Escalation-Exploits-Pack/
https://github.com/xairy/kernel-exploits

- Micropoor