Ubuntu\_26 =

{

"SEARCH": "ubuntu 2.6",

"RESULTS": [

{"Exploit":"Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/8478.sh","EDB-ID":8478},

{"Exploit":"Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/8572.c","EDB-ID":8572},

{"Exploit":"Linux Kernel 2.6.24\_16-23 / 2.6.27\_7-10 / 2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - set\_selection() UTF-8 Off-by-One Local Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/9083.c","EDB-ID":9083},

{"Exploit":"Linux Kernel 2.4.x / 2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu 8.10) (PPC) - 'sock\_sendpage()' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9545.c","EDB-ID":9545},

{"Exploit":"(Linux Kernel 2.6.34-rc3) ReiserFS (RedHat / Ubuntu 9.10) - 'xattr' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/12130.py","EDB-ID":12130},

{"Exploit":"Linux Kernel < 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32) - CAN BCM Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/14814.c","EDB-ID":14814},

{"Exploit":"Linux Kernel < 2.6.36-rc6 (RedHat / Ubuntu 10.04) - 'pktcdvd' Kernel Memory Disclosure (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15150.c","EDB-ID":15150},

{"Exploit":"Linux Kernel 2.6.37 (RedHat / Ubuntu 10.04) - 'Full-Nelson.c' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15704.c","EDB-ID":15704},

{"Exploit":"Linux Kernel < 2.6.34 (Ubuntu 10.10 x86) - 'CAP\_SYS\_ADMIN' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/local/15916.c","EDB-ID":15916},

{"Exploit":"Linux Kernel < 2.6.34 (Ubuntu 10.10 x86/x64) - 'CAP\_SYS\_ADMIN' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15944.c","EDB-ID":15944},

{"Exploit":"Linux Kernel < 2.6.36.2 (Ubuntu 10.04) - 'Half-Nelson.c' Econet Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/17787.c","EDB-ID":17787},

{"Exploit":"Linux Kernel 2.6.39 < 3.2.2 (Gentoo / Ubuntu x86/x64) - 'Mempodipper.c' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/18411.c","EDB-ID":18411},

{"Exploit":"Linux Kernel 2.6.32 (Ubuntu 10.04) - /proc Handling SUID Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/41770.txt","EDB-ID":41770},

{"Exploit":"Linux Kernel 2.6.20 / 2.6.24 / 2.6.27\_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora Core 10 / OpenSuse 11.1) - SCTP FWD Memory Corruption Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/8556.c","EDB-ID":8556}

]

}

Ubuntu\_26r=

{

"SEARCH": "ubuntu 2.6 remote",

"RESULTS": [

{"Exploit":"Linux Kernel 2.6.20 / 2.6.24 / 2.6.27\_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora Core 10 / OpenSuse 11.1) - SCTP FWD Memory Corruption Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/8556.c","EDB-ID":8556}

]

}

youpengs-MacBook-Air:NetSecure Bruce$ searchsploit -tj ubuntu 2.8

{

"SEARCH": "ubuntu 2.8",

"RESULTS": [

{"Exploit":"Systemd 228 (SUSE 12 SP2 / Ubuntu Touch 15.04) - Privilege Escalation (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/41171.txt","EDB-ID":41171}

]

}

searchsploit -tj ubuntu 2.8 remote

{

"SEARCH": "ubuntu 2.8 remote",

"RESULTS": [

]

}

searchsploit -tj ubuntu 2

{

"SEARCH": "ubuntu 2",

"RESULTS": [

{"Exploit":"Pure-FTPd 1.0.21 (CentOS 6.2 / Ubuntu 8.04) - Null Pointer Dereference Crash (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/20479.pl","EDB-ID":20479},

{"Exploit":"Linux Kernel 4.8.0-22 / 3.10.0-327 (Ubuntu 16.10 / RedHat) - 'keyctl' Null Pointer Dereference","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/40762.c","EDB-ID":40762},

{"Exploit":"Linux Kernel (Ubuntu 11.10/12.04) - binfmt\_script Stack Data Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/41767.txt","EDB-ID":41767},

{"Exploit":"Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/8478.sh","EDB-ID":8478},

{"Exploit":"Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/8572.c","EDB-ID":8572},

{"Exploit":"Linux Kernel 2.6.24\_16-23 / 2.6.27\_7-10 / 2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - set\_selection() UTF-8 Off-by-One Local Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/9083.c","EDB-ID":9083},

{"Exploit":"PulseAudio setuid (Ubuntu 9.04 / Slackware 12.2.0) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9208.txt","EDB-ID":9208},

{"Exploit":"Linux Kernel 2.4.x / 2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu 8.10) (PPC) - 'sock\_sendpage()' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9545.c","EDB-ID":9545},

{"Exploit":"(Linux Kernel 2.6.34-rc3) ReiserFS (RedHat / Ubuntu 9.10) - 'xattr' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/12130.py","EDB-ID":12130},

{"Exploit":"Linux PAM 1.1.0 (Ubuntu 9.10/10.04) - MOTD File Tampering Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/14339.sh","EDB-ID":14339},

{"Exploit":"Linux Kernel < 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32) - CAN BCM Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/14814.c","EDB-ID":14814},

{"Exploit":"mountall 2.15.2 (Ubuntu 10.04/10.10) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15074.sh","EDB-ID":15074},

{"Exploit":"Linux Kernel < 2.6.36-rc6 (RedHat / Ubuntu 10.04) - 'pktcdvd' Kernel Memory Disclosure (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15150.c","EDB-ID":15150},

{"Exploit":"Linux Kernel 2.6.37 (RedHat / Ubuntu 10.04) - 'Full-Nelson.c' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15704.c","EDB-ID":15704},

{"Exploit":"Linux Kernel < 2.6.34 (Ubuntu 10.10 x86) - 'CAP\_SYS\_ADMIN' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/local/15916.c","EDB-ID":15916},

{"Exploit":"Linux Kernel < 2.6.34 (Ubuntu 10.10 x86/x64) - 'CAP\_SYS\_ADMIN' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15944.c","EDB-ID":15944},

{"Exploit":"Linux Kernel < 2.6.36.2 (Ubuntu 10.04) - 'Half-Nelson.c' Econet Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/17787.c","EDB-ID":17787},

{"Exploit":"Acpid 1:2.0.10-1ubuntu2 (Ubuntu 11.04/11.10) - Boundary Crossing Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/18228.sh","EDB-ID":18228},

{"Exploit":"Linux Kernel 2.6.39 < 3.2.2 (Gentoo / Ubuntu x86/x64) - 'Mempodipper.c' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/18411.c","EDB-ID":18411},

{"Exploit":"Linux Kernel 3.7.10 (Ubuntu 12.10 x64) - 'sock\_diag\_handlers' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/24746.c","EDB-ID":24746},

{"Exploit":"Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG\_X86\_X32' Arbitrary Write Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/31346.c","EDB-ID":31346},

{"Exploit":"Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10) - 'CONFIG\_X86\_X32=y' Privilege Escalation (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/local/31347.c","EDB-ID":31347},

{"Exploit":"Linux Kernel 3.2.0-23 / 3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf\_swevent\_init' Privilege Escalation (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/33589.c","EDB-ID":33589},

{"Exploit":"Linux Kernel < 3.2.0-23 (Ubuntu 12.04 x64) - 'ptrace/sysret' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/34134.c","EDB-ID":34134},

{"Exploit":"Apport 2.14.1 (Ubuntu 14.04.2) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/36782.sh","EDB-ID":36782},

{"Exploit":"usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/36820.txt","EDB-ID":36820},

{"Exploit":"Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/37292.c","EDB-ID":37292},

{"Exploit":"Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation (Access /etc/shadow)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/37293.txt","EDB-ID":37293},

{"Exploit":"Apport 2.19 (Ubuntu 15.04) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/38353.txt","EDB-ID":38353},

{"Exploit":"Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter target\_offset Out-of-Bounds Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/40049.c","EDB-ID":40049},

{"Exploit":"Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T\_SO\_SET\_REPLACE' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40489.txt","EDB-ID":40489},

{"Exploit":"Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40937.txt","EDB-ID":40937},

{"Exploit":"Google Chrome + Fedora 25 / Ubuntu 16.04 - 'tracker-extract' / 'gnome-video-thumbnailer' + 'totem' Drive-By Download","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40943.txt","EDB-ID":40943},

{"Exploit":"Systemd 228 (SUSE 12 SP2 / Ubuntu Touch 15.04) - Privilege Escalation (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/41171.txt","EDB-ID":41171},

{"Exploit":"Linux Kernel 2.6.32 (Ubuntu 10.04) - /proc Handling SUID Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/41770.txt","EDB-ID":41770},

{"Exploit":"Linux Kernel 2.6.20 / 2.6.24 / 2.6.27\_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora Core 10 / OpenSuse 11.1) - SCTP FWD Memory Corruption Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/8556.c","EDB-ID":8556}

]

}

searchsploit -tj ubuntu 2 remote

{

"SEARCH": "ubuntu 2 remote",

"RESULTS": [

{"Exploit":"Linux Kernel 2.6.20 / 2.6.24 / 2.6.27\_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora Core 10 / OpenSuse 11.1) - SCTP FWD Memory Corruption Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/8556.c","EDB-ID":8556}

]

}

searchsploit -tj unix

{

"SEARCH": "unix",

"RESULTS": [

{"Exploit":"Linux Kernel < 2.4.36.9 / 2.6.27.5 - Unix Sockets Local Kernel Panic Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/7091.c","EDB-ID":7091},

{"Exploit":"Linux Kernel 2.6.31.4 - 'unix\_stream\_connect()' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/10022.c","EDB-ID":10022},

{"Exploit":"Linux Kernel 2.6.37 - Unix Sockets Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/15622.c","EDB-ID":15622},

{"Exploit":"Linux Kernel 2.0/2.1 (Digital UNIX 4.0 D / FreeBSD 2.2.4 / HP HP-UX 10.20/11.0 / IBM AIX 3.2.5 / NetBSD 1.2 / Solaris 2.5.1) - Smurf Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/19117.c","EDB-ID":19117},

{"Exploit":"Adobe Unix Acrobat Reader 4.0/5.0 - WWWLaunchNetscape Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/22846.pl","EDB-ID":22846},

{"Exploit":"Gauntlet Firewall for Unix 6.0 - SQL-GW Connection Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/23172.txt","EDB-ID":23172},

{"Exploit":"Common UNIX Printing System 1.2/1.3 SNMP - 'asn1\_get\_string()' Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/30898.pl","EDB-ID":30898},

{"Exploit":"Tru64 UNIX 4.0g - /usr/bin/at Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/tru64/local/281.c","EDB-ID":281},

{"Exploit":"UNIX 7th Edition /bin/mkdir - Local Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/302.c","EDB-ID":302},

{"Exploit":"SCO Unixware 7.1.3 - (ptrace) Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/1534.c","EDB-ID":1534},

{"Exploit":"Tru64 UNIX 5.0 (Rev. 910) - rdist NLSPATH Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/tru64/local/1624.pl","EDB-ID":1624},

{"Exploit":"Tru64 UNIX 5.0 (Rev. 910) - edauth NLSPATH Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/tru64/local/1625.pl","EDB-ID":1625},

{"Exploit":"SCO UnixWare < 7.1.4 p534589 - 'pkgadd' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/5355.sh","EDB-ID":5355},

{"Exploit":"SCO UnixWare Reliant HA 1.1.4 - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/5356.c","EDB-ID":5356},

{"Exploit":"SCO UnixWare Merge - 'mcd' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/5357.c","EDB-ID":5357},

{"Exploit":"Digital UNIX 4.0/4.0 B/4.0 D - SUID/SGID Core File","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19068.txt","EDB-ID":19068},

{"Exploit":"HP HP-UX 10.20/11.0 / IBM AIX 4.3 / SCO Unixware 7.0 / Sun Solaris 2.6 - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19108.txt","EDB-ID":19108},

{"Exploit":"FreeBSD 3.0 - UNIX-domain panic","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19130.c","EDB-ID":19130},

{"Exploit":"Sun Solaris 2.5.1 PAM & unix\_scheme - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/solaris/local/19158.c","EDB-ID":19158},

{"Exploit":"BSD/OS 2.1 / Caldera UnixWare 7/7.1.0 / FreeBSD 1.1.5.1/2.0 / HP HP-UX 10.34 / IBM AIX 4.2 / SGI IRIX 6.3 / SunOS 4.1.4 - libXt library Exploit (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19200.c","EDB-ID":19200},

{"Exploit":"BSD/OS 2.1 / Caldera UnixWare 7/7.1.0 / FreeBSD 1.1.5.1/2.0 / HP HP-UX 10.34 / IBM AIX 4.2 / SGI IRIX 6.3 / SunOS 4.1.4 - libXt library Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19201.c","EDB-ID":19201},

{"Exploit":"BSD/OS 2.1 / Caldera UnixWare 7/7.1.0 / FreeBSD 1.1.5.1/2.0 / HP HP-UX 10.34 / IBM AIX 4.2 / SGI IRIX 6.3 / SunOS 4.1.4 - libXt library Exploit (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19202.c","EDB-ID":19202},

{"Exploit":"BSD/OS 2.1 / DG/UX 4.0 / Debian 0.93 / Digital UNIX 4.0 B / FreeBSD 2.1.5 / HP-UX 10.34 / IBM AIX 4.1.5 / NetBSD 1.0/1.1 / NeXTstep 4.0 / SGI IRIX 6.3 / SunOS 4.1.4 - rlogin Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19203.c","EDB-ID":19203},

{"Exploit":"Rational Software ClearCase for Unix 3.2 - ClearCase SUID","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19429.sh","EDB-ID":19429},

{"Exploit":"DIGITAL UNIX 4.0 d/e/f / AIX 4.3.2 / CDE 2.1 / IRIX 6.5.14 / Solaris 7.0 - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/local/19497.c","EDB-ID":19497},

{"Exploit":"DIGITAL UNIX 4.0 d/f / AIX 4.3.2 / CDE 2.1 / IRIX 6.5.14 / Solaris 7.0 / SunOS 4.1.4 - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19501.c","EDB-ID":19501},

{"Exploit":"SCO Unixware 7.0/7.0.1/7.1/7.1.1 - Privileged Program Debugging","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19674.c","EDB-ID":19674},

{"Exploit":"SCO Unixware 7.0/7.0.1/7.1 - Xsco Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19641.c","EDB-ID":19641},

{"Exploit":"SCO Unixware 7.0 - xlock(1) (long 'Username') Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19642.c","EDB-ID":19642},

{"Exploit":"SCO Unixware 2.1/7.0/7.0.1/7.1/7.1.1 - su(1) Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19643.c","EDB-ID":19643},

{"Exploit":"SCO Unixware 7.0/7.0.1/7.1/7.1.1 - 'uidadmin' Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19654.pl","EDB-ID":19654},

{"Exploit":"SCO Unixware 7.0/7.0.1/7.1/7.1.1 - 'xauto' Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19656.c","EDB-ID":19656},

{"Exploit":"SCO Unixware 7.1 - '/var/mail' Permissions","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19657.txt","EDB-ID":19657},

{"Exploit":"SCO Unixware 7.1 - 'pkg' command Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19658.txt","EDB-ID":19658},

{"Exploit":"SCO Unixware 7.0/7.0.1/7.1/7.1.1 - 'coredump' Symlink","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19659.sh","EDB-ID":19659},

{"Exploit":"SCO Unixware 7.1 pkgcat - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19660.c","EDB-ID":19660},

{"Exploit":"SCO Unixware 7.1 pkginstall - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19661.c","EDB-ID":19661},

{"Exploit":"SCO Unixware 7.1/7.1.1 - ARCserver /tmp symlink","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/local/19752.txt","EDB-ID":19752},

{"Exploit":"Elm Development Group ELM 2.4/2.5.1 Mail for UNIX - (ELM) Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19971.c","EDB-ID":19971},

{"Exploit":"Elm Development Group ELM 2.4/2.5.1 Mail for UNIX - (ELM) Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19972.c","EDB-ID":19972},

{"Exploit":"Immunix OS 6.2 - LC glibc format string","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/immunix/local/20187.c","EDB-ID":20187},

{"Exploit":"GNOME esound 0.2.19 - Unix Domain Socket Race Condition","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/20212.c","EDB-ID":20212},

{"Exploit":"Siemens Reliant UNIX 5.4 - ppd -T Race Condition","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/20769.txt","EDB-ID":20769},

{"Exploit":"Immunix OS 6.2/7.0 / RedHat 5.2/6.2/7.0 / S.u.S.E 6.x/7.0/7.1 Man -S - Heap Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20843.txt","EDB-ID":20843},

{"Exploit":"Digital Unix 4.0 - MSGCHK Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/21105.c","EDB-ID":21105},

{"Exploit":"Digital Unix 4.0 - MSGCHK MH\_PROFILE Symbolic Link","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/21107.sh","EDB-ID":21107},

{"Exploit":"Caldera UnixWare 7.1.1 - WebTop SCOAdminReg.cgi Arbitrary Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unixware/local/21239.sh","EDB-ID":21239},

{"Exploit":"Caldera UnixWare 7.1.1 - Message Catalog Environment Variable Format String","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unixware/local/21284.c","EDB-ID":21284},

{"Exploit":"Cisco VPN Client for Unix 3.5.1 - Local Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21568.c","EDB-ID":21568},

{"Exploit":"OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40962.txt","EDB-ID":40962},

{"Exploit":"Ability Server 2.34 - FTP STOR Buffer Overflow (Unix Exploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/windows/remote/618.c","EDB-ID":618},

{"Exploit":"IBM AIX 3.2/4.1 & SCO Unixware 7.1.1 & SGI IRIX 5.3 & Sun Solaris 2.5.1 - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/19104.c","EDB-ID":19104},

{"Exploit":"Caldera OpenUnix 8.0/UnixWare 7.1.1 / HP HP-UX 11.0 / Solaris 7.0 / SunOS 4.1.4 - rpc.cmsd Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/19420.c","EDB-ID":19420},

{"Exploit":"Caldera OpenUnix 8.0/UnixWare 7.1.1 / HP HP-UX 11.0 / Solaris 7.0 / SunOS 4.1.4 - rpc.cmsd Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/19421.c","EDB-ID":19421},

{"Exploit":"SCO Unixware 7.1 - i2odialogd Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/remote/19680.c","EDB-ID":19680},

{"Exploit":"Unixware 7.0 - SCOhelp HTTP Server Format String","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/cgi/remote/20242.txt","EDB-ID":20242},

{"Exploit":"SCO UNIX 5 calserver - Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/remote/20620.c","EDB-ID":20620},

{"Exploit":"Adobe Acrobat Reader (UNIX) 5.0 6 / Xpdf 0.9x Hyperlinks - Arbitrary Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/22771.txt","EDB-ID":22771},

{"Exploit":"Linux/x86 & Unix/SPARC & IRIX/MIPS - execve /bin/sh Shellcode (141 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/shellcode/13467.c","EDB-ID":13467},

{"Exploit":"Linux/x86 & Unix/SPARC - execve /bin/sh Shellcode (80 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/shellcode/13468.c","EDB-ID":13468},

{"Exploit":"UnixWare - execve /bin/sh Shellcode (95 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unixware/shellcode/13503.txt","EDB-ID":13503}

]

}

searchsploit -tj unix remote

{

"SEARCH": "unix remote",

"RESULTS": [

{"Exploit":"Common UNIX Printing System 1.2/1.3 SNMP - 'asn1\_get\_string()' Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/30898.pl","EDB-ID":30898},

{"Exploit":"SCO Unixware 7.1 - i2odialogd Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/remote/19680.c","EDB-ID":19680},

{"Exploit":"SCO UNIX 5 calserver - Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sco/remote/20620.c","EDB-ID":20620}

]

}

searchsploit -tj freebsd

{

"SEARCH": "freebsd",

"RESULTS": [

{"Exploit":"FreeBSD 6.0 - (nfsd) Remote Kernel Panic Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/1540.pl","EDB-ID":1540},

{"Exploit":"FreeBSD 5.4 / 6.0 - (ptrace PT\_LWPINFO) Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/2524.c","EDB-ID":2524},

{"Exploit":"FreeBSD 6.1-RELEASE-p10 - (ftruncate) Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/2541.c","EDB-ID":2541},

{"Exploit":"FreeBSD 6.1-RELEASE-p10 - (scheduler) Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/2542.c","EDB-ID":2542},

{"Exploit":"FreeBSD 6.1 - (/dev/crypto) Local Kernel Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/2639.c","EDB-ID":2639},

{"Exploit":"FreeBSD 7.x - (Dumping Environment) Local Kernel Panic Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/8259.c","EDB-ID":8259},

{"Exploit":"FreeBSD 6/8 - (ata device) Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/9134.c","EDB-ID":9134},

{"Exploit":"FreeBSD 7.2 - (pecoff executable) Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/9206.c","EDB-ID":9206},

{"Exploit":"FreeBSD 7.2-RELEASE - SCTP Local Kernel Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/9373.c","EDB-ID":9373},

{"Exploit":"FreeBSD and OpenBSD 'ftpd' - Null Pointer Dereference Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/dos/11705.c","EDB-ID":11705},

{"Exploit":"FreeBSD 8.0 ftpd (FreeBSD-SA-10:05) - Off-By-One (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/12762.txt","EDB-ID":12762},

{"Exploit":"FreeBSD Kernel - mountnfs() Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/14003.c","EDB-ID":14003},

{"Exploit":"FreeBSD 8.1/7.3 - vm.pmap Kernel Local Race Condition","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/14947.txt","EDB-ID":14947},

{"Exploit":"FreeBSD 8.0 - Local Denial of Service (Forced Reboot)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/16064.c","EDB-ID":16064},

{"Exploit":"FreeBSD - UIPC socket heap Overflow (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/17908.sh","EDB-ID":17908},

{"Exploit":"Linux Kernel 2.0/2.1 (Digital UNIX 4.0 D / FreeBSD 2.2.4 / HP HP-UX 10.20/11.0 / IBM AIX 3.2.5 / NetBSD 1.2 / Solaris 2.5.1) - Smurf Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/19117.c","EDB-ID":19117},

{"Exploit":"Linux Kernel 2.3 (BSD/OS 4.0 / FreeBSD 3.2 / NetBSD 1.4) - Shared Memory Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/19423.c","EDB-ID":19423},

{"Exploit":"FreeBSD 5.0 / NetBSD 1.4.2 / OpenBSD 2.7 - setsockopt() Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/19488.c","EDB-ID":19488},

{"Exploit":"FreeBSD 3.0/3.1/3.2 vfs\_cache - Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/19505.c","EDB-ID":19505},

{"Exploit":"FreeBSD 3.4/4.0/5.0 / NetBSD 1.4 - Unaligned IP Option Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/19896.c","EDB-ID":19896},

{"Exploit":"FreeBSD 3.x/4.0/5.0 / NetBSD 1.4.1/1.4.2 / OpenBSD 2.x - Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/19982.c","EDB-ID":19982},

{"Exploit":"FreeBSD Kernel - SCTP Remote NULL Ptr Dereference Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/20226.c","EDB-ID":20226},

{"Exploit":"FreeBSD 2.x / HP-UX 9/10/11 / Kernel 2.0.3 / Windows NT 4.0/Server 2003 / NetBSD 1 - 'land.c' loopback Denial of Service (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/dos/20810.c","EDB-ID":20810},

{"Exploit":"FreeBSD 2.x / HP-UX 9/10/11 / Kernel 2.0.3 / Windows NT 4.0/Server 2003 / NetBSD 1 - 'land.c' loopback Denial of Service (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/dos/20811.cpp","EDB-ID":20811},

{"Exploit":"FreeBSD 2.x / HP-UX 9/10/11 / Kernel 2.0.3 / Windows NT 4.0/Server 2003 / NetBSD 1 - 'land.c' loopback Denial of Service (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/windows/dos/20812.c","EDB-ID":20812},

{"Exploit":"FreeBSD 2.x / HP-UX 9/10/11 / Kernel 2.0.3 / Windows NT 4.0/Server 2003 / NetBSD 1 - 'land.c' loopback Denial of Service (4)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/dos/20813.c","EDB-ID":20813},

{"Exploit":"FreeBSD 2.x / HP-UX 9/10/11 / Kernel 2.0.3 / Windows NT 4.0/Server 2003 / NetBSD 1 - 'land.c' loopback Denial of Service (5)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/windows/dos/20814.c","EDB-ID":20814},

{"Exploit":"FreeBSD 4.10/5.x - execve() Unaligned Memory Access Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/24233.c","EDB-ID":24233},

{"Exploit":"FreeBSD 9.1 ftpd - Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/24450.txt","EDB-ID":24450},

{"Exploit":"FreeBSD 5.x I386\_Set\_LDT() - Multiple Local Denial of Service Vulnerabilities","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/28648.c","EDB-ID":28648},

{"Exploit":"FreeBSD 5.5/6.x - Scheduler Policy Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/28812.c","EDB-ID":28812},

{"Exploit":"FreeBSD 6.0/6.1 Ftrucante - Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/28813.c","EDB-ID":28813},

{"Exploit":"FreeBSD 8.0 / OpenBSD 4.x - 'ftpd' Null Pointer Dereference Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/33708.c","EDB-ID":33708},

{"Exploit":"FreeBSD Kernel - Multiple Vulnerabilities","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/35938.txt","EDB-ID":35938},

{"Exploit":"FreeBSD SCTP ICMPv6 - Error Processing","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/39305.py","EDB-ID":39305},

{"Exploit":"FreeBSD 10.2 amd64 Kernel - amd64\_set\_ldt Heap Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86-64/dos/39570.c","EDB-ID":39570},

{"Exploit":"Firebird 1.0.2 FreeBSD 4.7-RELEASE - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/29.c","EDB-ID":29},

{"Exploit":"FreeBSD 3.5.1/4.2 - ports package xklock Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/286.c","EDB-ID":286},

{"Exploit":"FreeBSD 3.5.1/4.2 - Ports Package elvrec Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/287.c","EDB-ID":287},

{"Exploit":"FreeBSD TOP - Format String","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/739.c","EDB-ID":739},

{"Exploit":"Qpopper 4.0.8 (FreeBSD) - (poppassd) Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/1230.sh","EDB-ID":1230},

{"Exploit":"FreeBSD 4.x / < 5.4 - master.passwd Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/1311.c","EDB-ID":1311},

{"Exploit":"FreeBSD mcweject 0.9 (eject) - Buffer Overflow Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/3578.c","EDB-ID":3578},

{"Exploit":"FreeBSD 6x/7 protosw Kernel - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/7581.c","EDB-ID":7581},

{"Exploit":"FreeBSD 7.0-RELEASE Telnet Daemon - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/8055.txt","EDB-ID":8055},

{"Exploit":"FreeBSD 7.0/7.1 - (ktimer) Kernel Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/8261.c","EDB-ID":8261},

{"Exploit":"FreeBSD 7.0/7.1 vfs.usermount - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/9082.c","EDB-ID":9082},

{"Exploit":"FreeBSD 6.1 - kqueue() Null Pointer Dereference Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/9488.c","EDB-ID":9488},

{"Exploit":"FreeBSD 6.4 - pipeclose()/knlist\_cleardel() Race Condition","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/9859.c","EDB-ID":9859},

{"Exploit":"FreeBSD 7.2 VFS/devfs - Race Condition","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/9860.c","EDB-ID":9860},

{"Exploit":"FreeBSD 8.0 Run-Time Link-Editor (rtld) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/10255.txt","EDB-ID":10255},

{"Exploit":"FreeBSD Kernel - nfs\_mount() Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/14002.c","EDB-ID":14002},

{"Exploit":"FreeBSD - mbufs() sendfile Cache Poisoning Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/14688.c","EDB-ID":14688},

{"Exploit":"FreeBSD - 'pseudofs' Null Pointer Dereference Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/15206.c","EDB-ID":15206},

{"Exploit":"FreeBSD 5.4-RELEASE ftpd 6.00LS - sendfile kernel mem-leak Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/16119.c","EDB-ID":16119},

{"Exploit":"FreeBSD 6.4 - Netgraph Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/16951.c","EDB-ID":16951},

{"Exploit":"BSDI BSD/OS 2.1 / FreeBSD 2.1 / IBM AIX 4.2 / SGI IRIX 6.4 / Sun SunOS 4.1.3 - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19106.c","EDB-ID":19106},

{"Exploit":"FreeBSD 3.0 - UNIX-domain panic","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19130.c","EDB-ID":19130},

{"Exploit":"BSD/OS 2.1 / Caldera UnixWare 7/7.1.0 / FreeBSD 1.1.5.1/2.0 / HP HP-UX 10.34 / IBM AIX 4.2 / SGI IRIX 6.3 / SunOS 4.1.4 - libXt library Exploit (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19200.c","EDB-ID":19200},

{"Exploit":"BSD/OS 2.1 / Caldera UnixWare 7/7.1.0 / FreeBSD 1.1.5.1/2.0 / HP HP-UX 10.34 / IBM AIX 4.2 / SGI IRIX 6.3 / SunOS 4.1.4 - libXt library Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19201.c","EDB-ID":19201},

{"Exploit":"BSD/OS 2.1 / Caldera UnixWare 7/7.1.0 / FreeBSD 1.1.5.1/2.0 / HP HP-UX 10.34 / IBM AIX 4.2 / SGI IRIX 6.3 / SunOS 4.1.4 - libXt library Exploit (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19202.c","EDB-ID":19202},

{"Exploit":"BSD/OS 2.1 / DG/UX 4.0 / Debian 0.93 / Digital UNIX 4.0 B / FreeBSD 2.1.5 / HP-UX 10.34 / IBM AIX 4.1.5 / NetBSD 1.0/1.1 / NeXTstep 4.0 / SGI IRIX 6.3 / SunOS 4.1.4 - rlogin Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19203.c","EDB-ID":19203},

{"Exploit":"BSDI BSD/OS 4.0 /FreeBSD 3.2 /NetBSD 1.4 x86 / OpenBSD 2.5 - UFS Secure Level 1","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/19411.txt","EDB-ID":19411},

{"Exploit":"FreeBSD 3.1 / Solaris 2.6 - Domain Socket","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19346.c","EDB-ID":19346},

{"Exploit":"Debian 2.0/2.0 r5 / FreeBSD 3.2 / OpenBSD 2.4 / RedHat 5.2 i386 / S.u.S.E. 6.1 - Lsof Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19373.c","EDB-ID":19373},

{"Exploit":"Debian 2.0/2.0 r5 / FreeBSD 3.2 / OpenBSD 2.4 / RedHat 5.2 i386 / S.u.S.E. 6.1 - Lsof Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19374.c","EDB-ID":19374},

{"Exploit":"BSD/OS 2.1 / FreeBSD 2.1.5 / NeXTstep 4.x / IRIX 6.4 / SunOS 4.1.3/4.1.4 - lpr Buffer Overrun (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19544.c","EDB-ID":19544},

{"Exploit":"BSD/OS 2.1 / FreeBSD 2.1.5 / NeXTstep 4.x / IRIX 6.4 / SunOS 4.1.3/4.1.4 - lpr Buffer Overrun (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/19545.c","EDB-ID":19545},

{"Exploit":"BSD 2 / CND 1 / Sendmail 8.x / FreeBSD 2.1.x / HP-UX 10.x / AIX 4 / RedHat 4 - Sendmail Daemon","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/local/19556.sh","EDB-ID":19556},

{"Exploit":"FreeBSD 3.3/Linux Mandrake 7.0 - 'xsoldier' Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19676.c","EDB-ID":19676},

{"Exploit":"FreeBSD 3.3/Linux Mandrake 7.0 - 'xsoldier' Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19677.c","EDB-ID":19677},

{"Exploit":"FreeBSD 3.3 gdc - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19649.c","EDB-ID":19649},

{"Exploit":"FreeBSD 3.3 gdc - Symlink","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19650.txt","EDB-ID":19650},

{"Exploit":"FreeBSD 3.3 - Seyon setgid dialer","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19651.txt","EDB-ID":19651},

{"Exploit":"FreeBSD 3.3 xmindpath - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19652.c","EDB-ID":19652},

{"Exploit":"FreeBSD 3.3 angband - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19653.c","EDB-ID":19653},

{"Exploit":"FreeBSD 3.4 / NetBSD 1.4.1 / OpenBSD 2.6 - /proc File Sytem","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/19726.c","EDB-ID":19726},

{"Exploit":"FreeBSD 3.0/3.1/3.2/3.3/3.4 Asmon/Ascpu - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19756.txt","EDB-ID":19756},

{"Exploit":"FreeBSD 3.5/4.x - top Format String","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/20377.c","EDB-ID":20377},

{"Exploit":"FreeBSD 4.3/4.4 - Login Capabilities Privileged File Reading","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/21114.txt","EDB-ID":21114},

{"Exploit":"FreeBSD 4.4 - AIO Library Cross Process Memory Write","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/21176.c","EDB-ID":21176},

{"Exploit":"Apple Mac OSX 10.x / FreeBSD 4.x / OpenBSD 2.x / Solaris 2.5/2.6/7.0/8 - exec C Library Standard I/O File Descriptor Closure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/21407.c","EDB-ID":21407},

{"Exploit":"FreeBSD 4.x - Process Concealment Bypass","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/21462.sh","EDB-ID":21462},

{"Exploit":"FreeBSD 4.x / NetBSD 1.4.x/1.5.x/1.6 / OpenBSD 3 - pppd Arbitrary File Permission Modification Race Condition","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/21669.pl","EDB-ID":21669},

{"Exploit":"NetBSD/FreeBSD Port Systrace 1.x - Exit Routine Access Validation Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/local/24113.c","EDB-ID":24113},

{"Exploit":"FreeBSD 9.0 < 9.1 mmap/ptrace - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/26368.c","EDB-ID":26368},

{"Exploit":"FreeBSD 9 - Address Space Manipulation Privilege Escalation (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/26454.rb","EDB-ID":26454},

{"Exploit":"FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/28718.c","EDB-ID":28718},

{"Exploit":"FreeBSD 7.1 libc - Berkley DB Interface Uninitialized Memory Local Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/32946.c","EDB-ID":32946},

{"Exploit":"CVS (Linux/FreeBSD) - Remote Entry Line Heap Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/300.c","EDB-ID":300},

{"Exploit":"GNU Mailutils imap4d 0.6 (FreeBSD) - 'Search' Remote Format String","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/remote/1234.c","EDB-ID":1234},

{"Exploit":"FreeBSD Litespeed Web Server 4.0.17 with PHP - Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/remote/15723.c","EDB-ID":15723},

{"Exploit":"ProFTPd 1.3.2rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/16878.rb","EDB-ID":16878},

{"Exploit":"FreeBSD OpenSSH 3.5p1 - Remote Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/remote/17462.txt","EDB-ID":17462},

{"Exploit":"FreeBSD ftpd and ProFTPd on FreeBSD - Remote Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/remote/18181.txt","EDB-ID":18181},

{"Exploit":"FreeBSD Telnet Service - Encryption Key ID Buffer Overflow (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/remote/18369.rb","EDB-ID":18369},

{"Exploit":"BSD/OS 3.1/4.0.1 / FreeBSD 3.0/3.1/3.2 / RedHat Linux 6.0 - amd Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/remote/19478.c","EDB-ID":19478},

{"Exploit":"BSD/OS 3.1/4.0.1 / FreeBSD 3.0/3.1/3.2 / RedHat Linux 6.0 - amd Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/remote/19479.c","EDB-ID":19479},

{"Exploit":"FreeBSD 3.x/4.x - ipfw Filtering Evasion","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/remote/20593.txt","EDB-ID":20593},

{"Exploit":"FreeBSD 2.2-4.2 / NetBSD 1.2-4.5 / OpenBSD 2.x FTPd - glob() Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/remote/20731.c","EDB-ID":20731},

{"Exploit":"FreeBSD 4.2-stable ftpd - glob() Buffer Overflow Vulnerabilities","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/remote/20732.pl","EDB-ID":20732},

{"Exploit":"Linux Kernel 2.0.x/2.2.x/2.4.x (FreeBSD 4.x) - Network Device Driver Frame Padding Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/remote/22131.pl","EDB-ID":22131},

{"Exploit":"FreeBSD 4.8 - realpath() Off-by-One Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/remote/22976.pl","EDB-ID":22976},

{"Exploit":"FreeBSD i386 & AMD64 - Execve /bin/sh Shellcode (Anti-Debugging) (140 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/shellcode/13261.txt","EDB-ID":13261},

{"Exploit":"FreeBSD/x86 - setreuid\_ execve(pfctl -d) Shellcode (56 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13262.txt","EDB-ID":13262},

{"Exploit":"FreeBSD/x86 - connect back.send.exit /etc/passwd Shellcode (112 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13263.txt","EDB-ID":13263},

{"Exploit":"FreeBSD/x86 - kill all processes Shellcode (12 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13264.txt","EDB-ID":13264},

{"Exploit":"FreeBSD/x86 - rev connect\_ recv\_ jmp\_ return results Shellcode (90 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13265.c","EDB-ID":13265},

{"Exploit":"FreeBSD/x86 - /bin/cat /etc/master.passwd Null Free Shellcode (65 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13266.asm","EDB-ID":13266},

{"Exploit":"FreeBSD/x86 - reverse portbind 127.0.0.1:8000 /bin/sh Shellcode (89 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13267.asm","EDB-ID":13267},

{"Exploit":"FreeBSD/x86 - setuid(0); execve(ipf -Fa); Shellcode (57 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13268.asm","EDB-ID":13268},

{"Exploit":"FreeBSD/x86 - encrypted Shellcode /bin/sh (48 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13269.c","EDB-ID":13269},

{"Exploit":"FreeBSD/x86 - portbind 4883 with auth Shellcode (222 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13270.c","EDB-ID":13270},

{"Exploit":"FreeBSD/x86 - reboot(RB\_AUTOBOOT) Shellcode (7 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13271.c","EDB-ID":13271},

{"Exploit":"FreeBSD/x86 - execve /bin/sh Shellcode (23 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13272.c","EDB-ID":13272},

{"Exploit":"FreeBSD/x86 - execve /bin/sh Shellcode (2) (23 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13273.c","EDB-ID":13273},

{"Exploit":"FreeBSD/x86 - execve /bin/sh Shellcode (37 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13274.c","EDB-ID":13274},

{"Exploit":"FreeBSD/x86 - kldload /tmp/o.o Shellcode (74 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13275.c","EDB-ID":13275},

{"Exploit":"FreeBSD/x86 - chown 0:0 \_ chmod 6755 & execve /tmp/sh Shellcode (44 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13276.c","EDB-ID":13276},

{"Exploit":"FreeBSD/x86 - execve /tmp/sh Shellcode (34 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13277.c","EDB-ID":13277},

{"Exploit":"FreeBSD/x86 - connect (Port 31337) Shellcode (102 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13278.asm","EDB-ID":13278},

{"Exploit":"FreeBSD/x86-64 - exec(\_/bin/sh\_) Shellcode (31 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86-64/shellcode/13279.c","EDB-ID":13279},

{"Exploit":"FreeBSD/x86-64 - execve /bin/sh Shellcode (34 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86-64/shellcode/13280.c","EDB-ID":13280},

{"Exploit":"FreeBSD/x86 - portbind (Port 1337) Shellcode (167 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/13570.c","EDB-ID":13570},

{"Exploit":"FreeBSD/x86 - connect back Shellcode (81 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd\_x86/shellcode/16025.c","EDB-ID":16025}

]

}

searchsploit -tj freebsd remote

{

"SEARCH": "freebsd remote",

"RESULTS": [

{"Exploit":"FreeBSD 6.0 - (nfsd) Remote Kernel Panic Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/1540.pl","EDB-ID":1540},

{"Exploit":"FreeBSD Kernel - SCTP Remote NULL Ptr Dereference Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/20226.c","EDB-ID":20226},

{"Exploit":"FreeBSD 9.1 ftpd - Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/dos/24450.txt","EDB-ID":24450},

{"Exploit":"CVS (Linux/FreeBSD) - Remote Entry Line Heap Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/300.c","EDB-ID":300},

{"Exploit":"GNU Mailutils imap4d 0.6 (FreeBSD) - 'Search' Remote Format String","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/remote/1234.c","EDB-ID":1234},

{"Exploit":"FreeBSD Litespeed Web Server 4.0.17 with PHP - Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/remote/15723.c","EDB-ID":15723},

{"Exploit":"FreeBSD OpenSSH 3.5p1 - Remote Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/remote/17462.txt","EDB-ID":17462},

{"Exploit":"FreeBSD ftpd and ProFTPd on FreeBSD - Remote Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/remote/18181.txt","EDB-ID":18181}

]

}

searchsploit -tj linux

{

"SEARCH": "linux",

"RESULTS": [

{"Exploit":"Apache 2.0.44 (Linux) - Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/11.c","EDB-ID":11},

{"Exploit":"Linux Kernel 2.4.20 - 'decode\_fh' Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/68.c","EDB-ID":68},

{"Exploit":"Slackware Linux - /usr/bin/ppp-off Insecure /tmp Call Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/185.sh","EDB-ID":185},

{"Exploit":"Linux Kernel 2.6.3 - 'setsockopt' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/274.c","EDB-ID":274},

{"Exploit":"Linux Kernel 2.4.x / 2.6.x - Assembler Inline Function Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/306.c","EDB-ID":306},

{"Exploit":"Microsoft Messenger (Linux) - Denial of Service (MS03-043)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/windows/dos/385.c","EDB-ID":385},

{"Exploit":"Linux Kernel 2.4.28 / 2.6.9 - 'scm\_send Local' Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/685.c","EDB-ID":685},

{"Exploit":"Linux Kernel 2.6.9 / 2.4.22-28 - 'igmp.c' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/686.c","EDB-ID":686},

{"Exploit":"Linux Kernel 2.4.28 / 2.6.9 - vc\_resize int Local Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/690.c","EDB-ID":690},

{"Exploit":"Linux Kernel 2.4.28 / 2.6.9 - Memory Leak Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/691.c","EDB-ID":691},

{"Exploit":"Linux Kernel 2.4.28 / 2.6.9 - 'ip\_options\_get' Local Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/692.c","EDB-ID":692},

{"Exploit":"Linux Kernel 2.6.10 - Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/904.c","EDB-ID":904},

{"Exploit":"Linux Kernel PPC64/IA64 (AIO) - Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/911.c","EDB-ID":911},

{"Exploit":"Linux Kernel 2.6.12-rc4 - 'ioctl\_by\_bdev' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/998.c","EDB-ID":998},

{"Exploit":"Linux Kernel 2.6.x - 'sys\_timer\_create()' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/1657.asm","EDB-ID":1657},

{"Exploit":"Linux Kernel < 2.6.16.18 - Netfilter NAT SNMP Module Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/1880.c","EDB-ID":1880},

{"Exploit":"Linux Omnikey Cardman 4040 Driver - Local Buffer Overflow (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/3441.c","EDB-ID":3441},

{"Exploit":"Linux Kernel 2.6.21.1 - IPv6 Jumbo Bug Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/4893.c","EDB-ID":4893},

{"Exploit":"Linux Kernel < 2.4.36.9 / 2.6.27.5 - Unix Sockets Local Kernel Panic Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/7091.c","EDB-ID":7091},

{"Exploit":"Linux Kernel 2.6.27.8 - ATMSVC Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/7405.c","EDB-ID":7405},

{"Exploit":"Linux Kernel 2.6.27.7-generic / 2.6.18 / 2.6.24-1 - Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/7454.c","EDB-ID":7454},

{"Exploit":"Psi Jabber Client (Windows / Linux) - (8010/tcp) Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/dos/7555.py","EDB-ID":7555},

{"Exploit":"Linux Kernel < 2.6.30.5 - 'cfg80211' Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/9442.c","EDB-ID":9442},

{"Exploit":"Linux Kernel 2.6.x - 'fput()' Null Pointer Dereference Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/10017.c","EDB-ID":10017},

{"Exploit":"Linux Kernel 2.6.31.4 - 'unix\_stream\_connect()' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/10022.c","EDB-ID":10022},

{"Exploit":"Linux Kernel < 2.6.31-rc4 - 'nfs4\_proc\_lock()' Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/10202.c","EDB-ID":10202},

{"Exploit":"VideoLAN VLC Media Player 1.0.3 (OSX/Linux) - RTSP Buffer Overflow (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/dos/10334.py","EDB-ID":10334},

{"Exploit":"Linux Kernel 2.6.33.3 - SCTP INIT Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/14594.py","EDB-ID":14594},

{"Exploit":"Linux Kernel 2.6.37 - 'setup\_arg\_pages()' Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/15619.c","EDB-ID":15619},

{"Exploit":"Linux Kernel 2.6.37 - Unix Sockets Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/15622.c","EDB-ID":15622},

{"Exploit":"RedHat Linux - Stickiness of /tmp Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/16216.txt","EDB-ID":16216},

{"Exploit":"Linux Kernel 2.6.37 - Local Kernel Denial of Service (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/16263.c","EDB-ID":16263},

{"Exploit":"Linux Kernel < 2.6.37-rc2 - 'TCP\_MAXSEG' Kernel Panic Denial of Service (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/16952.c","EDB-ID":16952},

{"Exploit":"Linux NTP query client 4.2.6p1 - Heap Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/16960.txt","EDB-ID":16960},

{"Exploit":"Linux 2.6.37-rc1 - serial\_core TIOCGICOUNT Leak Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/16973.c","EDB-ID":16973},

{"Exploit":"Conky Linux 1.8.0 - Local Denial of Service (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/17400.c","EDB-ID":17400},

{"Exploit":"Linux Kernel 3.0.0 - 'perf\_count\_sw\_cpu\_clock' event Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/17769.c","EDB-ID":17769},

{"Exploit":"Linux 2.6.36 IGMP - Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/18378.c","EDB-ID":18378},

{"Exploit":"Linux Kernel 2.0 / 2.1 - Send a SIGIO Signal To Any Process","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19085.c","EDB-ID":19085},

{"Exploit":"Linux Kernel 2.0/2.1 (Digital UNIX 4.0 D / FreeBSD 2.2.4 / HP HP-UX 10.20/11.0 / IBM AIX 3.2.5 / NetBSD 1.2 / Solaris 2.5.1) - Smurf Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/19117.c","EDB-ID":19117},

{"Exploit":"Linux Kernel 2.2 / 2.3 / Debian Linux 2.1 / RedHat Linux 6.0 / S.u.S.E. Linux 6.1 - IP Options","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19241.c","EDB-ID":19241},

{"Exploit":"Linux Kernel 2.0 / 2.1 / 2.2 - autofs Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19250.txt","EDB-ID":19250},

{"Exploit":"Linux Kernel 2.0 - TCP Port Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19271.c","EDB-ID":19271},

{"Exploit":"Linux Kernel 2.2 - 'ldd core' Force Reboot","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19272.txt","EDB-ID":19272},

{"Exploit":"Linux Kernel 2.0 Sendmail - Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19282.c","EDB-ID":19282},

{"Exploit":"Linux Kernel 2.0.33 - IP Fragment Overlap","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19301.c","EDB-ID":19301},

{"Exploit":"Linux Kernel 2.0 / 2.0.33 - i\_count Overflow (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19308.c","EDB-ID":19308},

{"Exploit":"Linux Kernel 2.3 (BSD/OS 4.0 / FreeBSD 3.2 / NetBSD 1.4) - Shared Memory Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/dos/19423.c","EDB-ID":19423},

{"Exploit":"S.u.S.E. Linux 6.2 / Slackware Linux 3.2/3.6 - identd Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19463.c","EDB-ID":19463},

{"Exploit":"Linux Kernel 2.0.x (Debian 2.1 / RedHat 5.2) - Packet Length with Options","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19675.c","EDB-ID":19675},

{"Exploit":"Linux Kernel 3.2.24 - 'fs/eventpoll.c' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19605.c","EDB-ID":19605},

{"Exploit":"Linux Kernel 2.2.12/2.2.14/2.3.99 (RedHat 6.x) - Socket Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19818.c","EDB-ID":19818},

{"Exploit":"RedHat Linux 6.x - X Font Server Denial of Service / Buffer Overflow Vulnerabilities","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19850.c","EDB-ID":19850},

{"Exploit":"OpenLinux 2.3/2.4 / RedHat 6.0/6.1 / SCO eServer 2.3 - Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/20026.c","EDB-ID":20026},

{"Exploit":"RedHat Linux 6.1 i386 - Tmpwatch Recursive Write Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/20217.c","EDB-ID":20217},

{"Exploit":"RedHat Linux 7.0 - Roaring Penguin PPPoE Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/20494.pl","EDB-ID":20494},

{"Exploit":"(Linux Kernel) ReiserFS 3.5.28 - Denial of Service (Possible Code Execution)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/20535.txt","EDB-ID":20535},

{"Exploit":"Linux Kernel 2.1.89 / 2.2.x - Zero-Length Fragment","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/20566.c","EDB-ID":20566},

{"Exploit":"Trend Micro Interscan VirusWall (Linux) 3.0.1 - Multiple Program Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/20750.txt","EDB-ID":20750},

{"Exploit":"HP-UX 11 / Linux Kernel 2.4 / Windows 2000/NT 4.0 / IRIX 6.5 - Small TCP MSS Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/dos/20997.c","EDB-ID":20997},

{"Exploit":"Linux - SELinux W+X Protection Bypass via AIO","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/40419.c","EDB-ID":40419},

{"Exploit":"Linux Kernel 2.2 / 2.4 - Deep Symbolic Link Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/21122.sh","EDB-ID":21122},

{"Exploit":"Linux Kernel 2.4.18/19 - Privileged File Descriptor Resource Exhaustion","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/21598.c","EDB-ID":21598},

{"Exploit":"Linux Kernel 2.2 - 'mmap()' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/22105.c","EDB-ID":22105},

{"Exploit":"ViRobot Linux Server 2.0 - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/23045.pl","EDB-ID":23045},

{"Exploit":"MySQL (Linux) - Stack Based Buffer Overrun (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/23075.pl","EDB-ID":23075},

{"Exploit":"MySQL (Linux) - Heap Based Overrun (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/23076.pl","EDB-ID":23076},

{"Exploit":"Linux Kernel 2.4 / 2.6 - Sigqueue Blocking Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/23946.c","EDB-ID":23946},

{"Exploit":"Linux Kernel 2.6.x - IPTables Logging Rules Integer Underflow Remote (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/24696.c","EDB-ID":24696},

{"Exploit":"Linux Kernel - 'SCTP\_GET\_ASSOC\_STATS()' Stack Based Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/24747.c","EDB-ID":24747},

{"Exploit":"Linux Kernel 2.4.x / 2.6.x - Local Denial of Service / Memory Disclosure Vulnerabilities","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/24777.txt","EDB-ID":24777},

{"Exploit":"Linux Kernel 2.6.x - 'AIO\_Free\_Ring' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/24804.c","EDB-ID":24804},

{"Exploit":"UML\_Utilities User-Mode Linux - uml\_utilities 20030903 UML\_Net Slip Network Interface Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/25017.txt","EDB-ID":25017},

{"Exploit":"Linux Kernel 2.6.32-642 / 3.16.0-4 - 'inode' Integer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/40819.c","EDB-ID":40819},

{"Exploit":"Linux Kernel 2.4.x / 2.6.x - Multiple Unspecified ISO9660 Filesystem Handling Vulnerabilities","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/25234.sh","EDB-ID":25234},

{"Exploit":"Linux Kernel 2.4.x / 2.6.x - BlueTooth Signed Buffer Index (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/25287.c","EDB-ID":25287},

{"Exploit":"Linux Kernel 2.6.10 - File Lock Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/25322.c","EDB-ID":25322},

{"Exploit":"Linux Kernel 2.2.x / 2.3.x / 2.4.x / 2.5.x / 2.6.x - ELF Core Dump Local Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/25647.sh","EDB-ID":25647},

{"Exploit":"Linux Kernel 2.6.x - SCSI ProcFS Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/26248.sh","EDB-ID":26248},

{"Exploit":"Linux Kernel 2.6.x - IPv6 Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/26382.c","EDB-ID":26382},

{"Exploit":"Linux Kernel 2.6.x - Sysctl Unregistration Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/26489.c","EDB-ID":26489},

{"Exploit":"Linux Kernel 2.6.x - Time\_Out\_Leases PrintK Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/26648.c","EDB-ID":26648},

{"Exploit":"Linux Kernel 2.6.x - File Lock Lease Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/26749.c","EDB-ID":26749},

{"Exploit":"Linux Kernel 2.6.x - INVALIDATE\_INODE\_PAGES2 Local Integer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/26811.c","EDB-ID":26811},

{"Exploit":"Linux Kernel 2.6.x - SET\_MEMPOLICY Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/27031.c","EDB-ID":27031},

{"Exploit":"Linux Kernel 2.6.x - Proc dentry\_unused Corruption Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/27925.txt","EDB-ID":27925},

{"Exploit":"Linux Kernel 2.6.17.7 - NFS and EXT3 Combination Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/28358.txt","EDB-ID":28358},

{"Exploit":"Linux-HA Heartbeat 2.0.6 - Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/28386.txt","EDB-ID":28386},

{"Exploit":"Evince PDF Reader 2.32.0.145 (Windows) / 3.4.0 (Linux) - Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/dos/28679.txt","EDB-ID":28679},

{"Exploit":"Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/28895.txt","EDB-ID":28895},

{"Exploit":"Linux Kernel 2.6.x - 'ISO9660' Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/28912.txt","EDB-ID":28912},

{"Exploit":"Linux Kernel 2.6.x - Audit Subsystems Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/29683.txt","EDB-ID":29683},

{"Exploit":"Linux Kernel 2.6.x - IPv6\_SockGlue.c Null Pointer Dereference Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/29781.c","EDB-ID":29781},

{"Exploit":"Linux Kernel 2.6.x - AppleTalk ATalk\_Sum\_SKB Function Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/29826.txt","EDB-ID":29826},

{"Exploit":"Linux Kernel 2.6.x - NETLINK\_FIB\_LOOKUP Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/29916.c","EDB-ID":29916},

{"Exploit":"Linux Kernel 2.6.x - VFat Compat IOCTLS Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/30080.c","EDB-ID":30080},

{"Exploit":"Linux Kernel 2.6.22 - IPv6 Hop-By-Hop Header Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/30902.c","EDB-ID":30902},

{"Exploit":"Linux Kernel 3.4 < 3.13.2 - recvmmsg x32 compat (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/31305.c","EDB-ID":31305},

{"Exploit":"Linux Kernel 2.6.9 < 2.6.25 (RHEL 4) - utrace and ptrace Local Denial of Service (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/31965.c","EDB-ID":31965},

{"Exploit":"Linux Kernel 2.6.9 < 2.6.25 (RHEL 4) - utrace and ptrace Local Denial of Service (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/31966.c","EDB-ID":31966},

{"Exploit":"Linux Kernel 2.6.x - 'add\_to\_page\_cache\_lru()' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/32384.txt","EDB-ID":32384},

{"Exploit":"Linux Kernel (Fedora 8/9) - 'utrace\_control' Null Pointer Dereference Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/32451.txt","EDB-ID":32451},

{"Exploit":"Linux Kernel 2.6.x - 'qdisc\_run()' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/32682.c","EDB-ID":32682},

{"Exploit":"Linux Kernel 2.6.x - 'make\_indexed\_dir()' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/32775.txt","EDB-ID":32775},

{"Exploit":"Linux Kernel 2.6.x - Cloned Process 'CLONE\_PARENT' Local Origin Validation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/32815.c","EDB-ID":32815},

{"Exploit":"Linux group\_info refcounter - Overflow Memory Corruption","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/32926.c","EDB-ID":32926},

{"Exploit":"Linux Kernel 2.6.x - 'splice(2)' Double Lock Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/33015.c","EDB-ID":33015},

{"Exploit":"Linux Kernel 2.6.x - '/proc/iomem' Sparc64 Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/33043.txt","EDB-ID":33043},

{"Exploit":"Linux Kernel 2.6.30 - 'tun\_chr\_pool()' Null Pointer Dereference","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/33088.txt","EDB-ID":33088},

{"Exploit":"Linux Kernel 2.6.x - 'posix-timers.c' Null Pointer Dereference Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/33148.c","EDB-ID":33148},

{"Exploit":"Linux Kernel 2.6.x - 'drivers/char/tty\_ldisc.c' Null Pointer Dereference Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/33193.c","EDB-ID":33193},

{"Exploit":"Linux Kernel 2.6.31 - 'perf\_counter\_open()' Local Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/33228.txt","EDB-ID":33228},

{"Exploit":"Linux Kernel 2.6.x - '/drivers/net/r8169.c' Out-of-IOMMU Error Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/33289.txt","EDB-ID":33289},

{"Exploit":"Linux Kernel 2.6.x - KVM 'pit\_ioport\_read()' Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/33592.txt","EDB-ID":33592},

{"Exploit":"Linux Kernel 2.6.x - 'net/ipv6/ip6\_output.c' Null Pointer Dereference Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/33635.c","EDB-ID":33635},

{"Exploit":"Linux Kernel 2.6.x (x64) - Personality Handling Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/dos/33585.txt","EDB-ID":33585},

{"Exploit":"Linux Kernel 2.6.34 - 'find\_keyring\_by\_name()' Local Memory Corruption","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/33886.txt","EDB-ID":33886},

{"Exploit":"Linux Kernel 2.6.x - 'inotify\_init()' Memory Leak Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/35013.c","EDB-ID":35013},

{"Exploit":"Linux Kernel 2.6.x - epoll Nested Structures Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/35403.c","EDB-ID":35403},

{"Exploit":"Linux Kernel 2.6.x - fs/eventpoll.c epoll Data Structure File Descriptor Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/35404.c","EDB-ID":35404},

{"Exploit":"Linux Kernel 2.6.x - 'inotify\_init1()' Double-Free Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/35600.c","EDB-ID":35600},

{"Exploit":"Linux Kernel 2.6.x - KSM Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/35820.c","EDB-ID":35820},

{"Exploit":"Linux Kernel 2.6.26 - Auerswald USB Device Driver Buffer Overflow (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/35957.txt","EDB-ID":35957},

{"Exploit":"Linux Kernel 3.17.5 - IRET Instruction #SS Fault Handling Crash (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/dos/36266.c","EDB-ID":36266},

{"Exploit":"Linux Kernel 3.15.6 - PPP-over-L2TP Socket Level Handling Crash (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/36267.c","EDB-ID":36267},

{"Exploit":"Linux Kernel 3.16.3 - Associative Array Garbage Collection Crash (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/36268.c","EDB-ID":36268},

{"Exploit":"Linux Kernel 2.6.35 - Network Namespace Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/36425.txt","EDB-ID":36425},

{"Exploit":"Linux Kernel 3.1.8 - KVM Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/36545.txt","EDB-ID":36545},

{"Exploit":"Linux Kernel 3.13 / 3.14 (Ubuntu) - 'splice()' System Call Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/36743.c","EDB-ID":36743},

{"Exploit":"Adobe Flash (Linux x64) - Bad Dereference at 0x23c","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/dos/37868.txt","EDB-ID":37868},

{"Exploit":"Linux Kernel 3.3.5 - Btrfs CRC32C feature Infinite Loop Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/38132.py","EDB-ID":38132},

{"Exploit":"Linux Kernel 3.2.1 - Tracing Multiple Local Denial of Service Vulnerabilities","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/38465.txt","EDB-ID":38465},

{"Exploit":"Linux Kernel 3.0.5 - 'test\_root()' Function Local Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/38589.c","EDB-ID":38589},

{"Exploit":"Linux Kernel 3.x / 4.x - prima WLAN Driver Heap Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39308.c","EDB-ID":39308},

{"Exploit":"Linux io\_submit L2TP sendmsg - Integer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39505.c","EDB-ID":39505},

{"Exploit":"Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'digi\_acceleport' Nullpointer Dereference","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39537.txt","EDB-ID":39537},

{"Exploit":"Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'Wacom' Multiple Nullpointer Dereferences","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39538.txt","EDB-ID":39538},

{"Exploit":"Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - visor (treo\_attach) Nullpointer Dereference","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39539.txt","EDB-ID":39539},

{"Exploit":"Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - visor clie\_5\_attach Nullpointer Dereference","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39540.txt","EDB-ID":39540},

{"Exploit":"Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'cypress\_m8' Nullpointer Dereference","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39542.txt","EDB-ID":39542},

{"Exploit":"Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'mct\_u232' Nullpointer Dereference","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39541.txt","EDB-ID":39541},

{"Exploit":"Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'cdc\_acm' Nullpointer Dereference","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39543.txt","EDB-ID":39543},

{"Exploit":"Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'aiptek' Nullpointer Dereference","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39544.txt","EDB-ID":39544},

{"Exploit":"Linux Kernel 3.10 / 3.18 / 4.4 - Netfilter IPT\_SO\_SET\_REPLACE Memory Corruption","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39545.txt","EDB-ID":39545},

{"Exploit":"Linux Kernel 3.10.0-229.x (CentOS / RHEL 7.1) - 'snd-usb-audio' Crash (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39555.txt","EDB-ID":39555},

{"Exploit":"Linux Kernel 3.10.0-229.x (CentOS / RHEL 7.1) - 'iowarrior' Driver Crash (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39556.txt","EDB-ID":39556},

{"Exploit":"Linux (x86) - Disable ASLR by Setting the RLIMIT\_STACK Resource to Unlimited","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/dos/39669.txt","EDB-ID":39669},

{"Exploit":"Linux Kernel (Ubuntu 16.04) - Reference Count Overflow Using BPF Maps","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/39773.txt","EDB-ID":39773},

{"Exploit":"Linux ARM/ARM64 - perf\_event\_open() Arbitrary Memory Read","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/dos/40182.txt","EDB-ID":40182},

{"Exploit":"Linux Kernel - TCP Related Read Use-After-Free","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/40731.c","EDB-ID":40731},

{"Exploit":"Linux Kernel 4.8.0-22 / 3.10.0-327 (Ubuntu 16.10 / RedHat) - 'keyctl' Null Pointer Dereference","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/40762.c","EDB-ID":40762},

{"Exploit":"Linux Kernel 3.10.0 (CentOS7) - Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/41350.c","EDB-ID":41350},

{"Exploit":"Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/41457.c","EDB-ID":41457},

{"Exploit":"Linux Kernel (Ubuntu 11.10/12.04) - binfmt\_script Stack Data Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/41767.txt","EDB-ID":41767},

{"Exploit":"Linux Kernel 2.2.x / 2.4.x (RedHat) - 'ptrace/kmod' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/3.c","EDB-ID":3},

{"Exploit":"Linux Kernel < 2.4.20 - Module Loader Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/12.c","EDB-ID":12},

{"Exploit":"Mandrake Linux 8.2 /usr/mail - Local Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40.pl","EDB-ID":40},

{"Exploit":"Linux Kernel 2.4.22 - 'do\_brk()' Privilege Escalation (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/129.asm","EDB-ID":129},

{"Exploit":"Linux Kernel 2.4.22 - 'do\_brk()' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/131.c","EDB-ID":131},

{"Exploit":"Linux Kernel 2.4.23 / 2.6.0 - 'do\_mremap()' Bound Checking Validator (PoC) (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/141.c","EDB-ID":141},

{"Exploit":"Linux Kernel 2.4.23 / 2.6.0 - 'do\_mremap()' Bound Checking Validator (PoC) (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/142.c","EDB-ID":142},

{"Exploit":"SuSE Linux 9.0 - YaST config Skribt Local Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/144.c","EDB-ID":144},

{"Exploit":"Linux Kernel 2.4.23 / 2.6.0 - 'do\_mremap()' Bound Checking Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/145.c","EDB-ID":145},

{"Exploit":"Linux Kernel 2.2.25 / 2.4.24 / 2.6.2 - 'mremap()' Validator (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/154.c","EDB-ID":154},

{"Exploit":"Linux Kernel 2.2.25 / 2.4.24 / 2.6.2 - 'mremap()' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/160.c","EDB-ID":160},

{"Exploit":"Seyon 2.1 rev. 4b i586-Linux - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/252.pl","EDB-ID":252},

{"Exploit":"Resolv+ (RESOLV\_HOST\_CONF) - Linux Library Local Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/317.txt","EDB-ID":317},

{"Exploit":"BSD & Linux umount - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/local/321.c","EDB-ID":321},

{"Exploit":"BSD & Linux lpr - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/325.c","EDB-ID":325},

{"Exploit":"Linux Kernel 2.4.26 - File Offset Pointer Handling Memory Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/375.c","EDB-ID":375},

{"Exploit":"Sendmail 8.11.x (Linux/i386) - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/411.c","EDB-ID":411},

{"Exploit":"Linux Kernel 2.4.27 / 2.6.8 - 'binfmt\_elf' Executable File Read Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/624.c","EDB-ID":624},

{"Exploit":"Linux Kernel 2.6.x < 2.6.7-rc3 (Slackware 9.1 / Debian 3.0) - 'sys\_chown()' Group Ownership Alteration Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/718.c","EDB-ID":718},

{"Exploit":"Linux Kernel 2.4.29-rc2 - 'uselib()' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/744.c","EDB-ID":744},

{"Exploit":"Linux Kernel 2.4 - 'uselib()' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/778.c","EDB-ID":778},

{"Exploit":"Linux ncpfs - Local Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/779.sh","EDB-ID":779},

{"Exploit":"Linux Kernel 2.4.x / 2.6.x - 'uselib()' Privilege Escalation (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/895.c","EDB-ID":895},

{"Exploit":"Aeon 0.2a - Local Linux Exploit (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/913.pl","EDB-ID":913},

{"Exploit":"Aeon 0.2a - Local Linux Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/914.c","EDB-ID":914},

{"Exploit":"Linux Kernel 2.4.x / 2.6.x - 'Bluez' BlueTooth Signed Buffer Index Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/926.c","EDB-ID":926},

{"Exploit":"MySQL 4.0.17 (Linux) - User-Defined Function (UDF) Dynamic Library Exploit (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/1181.c","EDB-ID":1181},

{"Exploit":"Qpopper 4.0.8 (Linux) - 'poppassd' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/1229.sh","EDB-ID":1229},

{"Exploit":"F-Secure Internet GateKeeper for Linux < 2.15.484 (and Gateway < 2.16) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/1297.py","EDB-ID":1297},

{"Exploit":"Linux chfn (SuSE 9.3 / 10) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/1299.sh","EDB-ID":1299},

{"Exploit":"Linux Kernel 2.6.9 < 2.6.11 (RHEL 4) - 'SYS\_EPoll\_Wait' Local Integer Overflow Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/1397.c","EDB-ID":1397},

{"Exploit":"MySQL 4.x/5.0 (Linux) - User-Defined Function (UDF) Dynamic Library Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/1518.c","EDB-ID":1518},

{"Exploit":"Linux Kernel 2.6.13 < 2.6.17.4 - 'sys\_prctl()' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/2004.c","EDB-ID":2004},

{"Exploit":"Linux Kernel 2.6.13 < 2.6.17.4 - 'sys\_prctl()' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/2005.c","EDB-ID":2005},

{"Exploit":"Linux Kernel 2.6.13 < 2.6.17.4 - 'sys\_prctl()' Privilege Escalation (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/2006.c","EDB-ID":2006},

{"Exploit":"Linux Kernel 2.6.13 < 2.6.17.4 - 'sys\_prctl()' Privilege Escalation (4)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/2011.sh","EDB-ID":2011},

{"Exploit":"Linux Kernel 2.6.17.4 - 'proc' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/2013.c","EDB-ID":2013},

{"Exploit":"Linux Kernel 2.6.13 < 2.6.17.4 - 'logrotate prctl()' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/2031.c","EDB-ID":2031},

{"Exploit":"GNU/Linux mbse-bbs 0.70.0 - Local Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/3154.c","EDB-ID":3154},

{"Exploit":"Nortel SSL VPN Linux Client 6.0.3 - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/3356.sh","EDB-ID":3356},

{"Exploit":"Linux Kernel 2.6.20 with DCCP Support - Memory Disclosure (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/3587.c","EDB-ID":3587},

{"Exploit":"Linux Kernel 2.6.20 with DCCP Support - Memory Disclosure (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/3595.c","EDB-ID":3595},

{"Exploit":"Linux Kernel < 2.6.20.2 - 'IPv6\_Getsockopt\_Sticky' Memory Leak (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/4172.c","EDB-ID":4172},

{"Exploit":"Linux Kernel 2.4 / 2.6 (x86-64) - System Call Emulation Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/4460.c","EDB-ID":4460},

{"Exploit":"Linux Kernel < 2.6.11.5 - BlueTooth Stack Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/4756.c","EDB-ID":4756},

{"Exploit":"Linux Kernel 2.6.17 < 2.6.24.1 - 'vmsplice' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/5092.c","EDB-ID":5092},

{"Exploit":"Linux Kernel 2.6.23 < 2.6.24 - 'vmsplice' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/5093.c","EDB-ID":5093},

{"Exploit":"Linux Kernel < 2.6.22 - 'ftruncate()/open()' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/6851.c","EDB-ID":6851},

{"Exploit":"Linux Kernel < 2.6.26.4 - SCTP Kernel Memory Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/7618.c","EDB-ID":7618},

{"Exploit":"Linux Kernel < 2.6.29 - 'exit\_notify()' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/8369.sh","EDB-ID":8369},

{"Exploit":"Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/8478.sh","EDB-ID":8478},

{"Exploit":"Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/8572.c","EDB-ID":8572},

{"Exploit":"Linux Kernel 2.6.x (Gentoo 2.6.29rc1) - 'ptrace\_attach' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/8673.c","EDB-ID":8673},

{"Exploit":"Linux Kernel 2.6.29 - 'ptrace\_attach()' Race Condition Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/8678.c","EDB-ID":8678},

{"Exploit":"Linux Kernel 2.6.24\_16-23 / 2.6.27\_7-10 / 2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - set\_selection() UTF-8 Off-by-One Local Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/9083.c","EDB-ID":9083},

{"Exploit":"Linux Kernel 2.6.30 < 2.6.30.1 / SELinux (RHEL 5) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9191.txt","EDB-ID":9191},

{"Exploit":"Linux Kernel 2.6.31-rc5 - sigaltstack 4-Byte Stack Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9352.c","EDB-ID":9352},

{"Exploit":"Linux Kernel < 2.6.14.6 - 'procfs' Kernel Memory Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9363.c","EDB-ID":9363},

{"Exploit":"Linux Kernel 2.x (RedHat) - 'sock\_sendpage()' Ring0 Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9435.txt","EDB-ID":9435},

{"Exploit":"Linux Kernel 2.x - 'sock\_sendpage()' Privilege Escalation (4)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9436.txt","EDB-ID":9436},

{"Exploit":"Linux Kernel 2.x (Android) - 'sock\_sendpage()' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/android/local/9477.txt","EDB-ID":9477},

{"Exploit":"Linux Kernel 2.4 / 2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock\_sendpage()' Ring0 Privilege Escalation (5)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9479.c","EDB-ID":9479},

{"Exploit":"Linux Kernel 2.6.31-rc7 - 'AF\_LLC getsockname' 5-Byte Stack Disclosure (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9513.c","EDB-ID":9513},

{"Exploit":"Linux Kernel 2.6.30 - 'atalk\_getname()' 8-bytes Stack Disclosure (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9521.c","EDB-ID":9521},

{"Exploit":"Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip\_append\_data()' Ring0 Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/local/9542.c","EDB-ID":9542},

{"Exploit":"Linux Kernel < 2.6.31-rc7 - 'AF\_IRDA' 29-Byte Stack Disclosure (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9543.c","EDB-ID":9543},

{"Exploit":"Linux Kernel 2.4.x / 2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu 8.10) (PPC) - 'sock\_sendpage()' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9545.c","EDB-ID":9545},

{"Exploit":"Linux Kernel < 2.6.19 (x86/x64) - 'udp\_sendmsg' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9574.txt","EDB-ID":9574},

{"Exploit":"Linux Kernel < 2.6.19 (Debian 4) - 'udp\_sendmsg' Privilege Escalation (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9575.c","EDB-ID":9575},

{"Exploit":"Linux Kernel 2.4 / 2.6 (Fedora 11) - 'sock\_sendpage()' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9598.txt","EDB-ID":9598},

{"Exploit":"Enlightenment - Linux Null PTR Dereference Exploit Framework","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9627.txt","EDB-ID":9627},

{"Exploit":"Linux Kernel 2.4 / 2.6 - 'sock\_sendpage()' Privilege Escalation (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9641.txt","EDB-ID":9641},

{"Exploit":"Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6.32-rc5 - 'pipe.c' Privilege Escalation (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/9844.py","EDB-ID":9844},

{"Exploit":"Linux PAM 1.1.0 (Ubuntu 9.10/10.04) - MOTD File Tampering Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/14273.sh","EDB-ID":14273},

{"Exploit":"Linux Kernel 2.6.32 - 'pipe.c' Privilege Escalation (4)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/10018.sh","EDB-ID":10018},

{"Exploit":"VMware Virtual 8086 - Linux Local Ring0 Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/local/10207.txt","EDB-ID":10207},

{"Exploit":"Linux Kernel 2.6.18 < 2.6.18-20 - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/10613.c","EDB-ID":10613},

{"Exploit":"(Linux Kernel 2.6.34-rc3) ReiserFS (RedHat / Ubuntu 9.10) - 'xattr' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/12130.py","EDB-ID":12130},

{"Exploit":"Linux PAM 1.1.0 (Ubuntu 9.10/10.04) - MOTD File Tampering Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/14339.sh","EDB-ID":14339},

{"Exploit":"Linux Kernel < 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32) - CAN BCM Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/14814.c","EDB-ID":14814},

{"Exploit":"Linux Kernel < 2.6.36-rc4-git2 (x86-64) - 'ia32syscall' Emulation Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/15023.c","EDB-ID":15023},

{"Exploit":"Linux Kernel 2.6.27 < 2.6.36 (RedHat x86-64) - 'compat' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/15024.c","EDB-ID":15024},

{"Exploit":"Linux Kernel < 2.6.36-rc6 (RedHat / Ubuntu 10.04) - 'pktcdvd' Kernel Memory Disclosure (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15150.c","EDB-ID":15150},

{"Exploit":"Linux Kernel 2.6.36-rc8 - 'RDS Protocol' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15285.c","EDB-ID":15285},

{"Exploit":"Linux Kernel 2.6.36 - VIDIOCSMICROCODE IOCTL Local Memory Overwrite","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15344.c","EDB-ID":15344},

{"Exploit":"Linux Kernel 2.4.0 - Stack Infoleaks","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15481.c","EDB-ID":15481},

{"Exploit":"Linux Kernel 2.6.37 (RedHat / Ubuntu 10.04) - 'Full-Nelson.c' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15704.c","EDB-ID":15704},

{"Exploit":"Linux Kernel < 2.6.37-rc2 - 'ACPI custom\_method' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15774.c","EDB-ID":15774},

{"Exploit":"Linux Kernel < 2.6.34 (Ubuntu 10.10 x86) - 'CAP\_SYS\_ADMIN' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/local/15916.c","EDB-ID":15916},

{"Exploit":"Linux Kernel < 2.6.34 (Ubuntu 10.10 x86/x64) - 'CAP\_SYS\_ADMIN' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/15944.c","EDB-ID":15944},

{"Exploit":"Linux Kernel (Solaris 10 / < 5.10 138888-01) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/solaris/local/15962.c","EDB-ID":15962},

{"Exploit":"Linux Kernel 4.6.3 (x86) - 'Netfilter' Privilege Escalation (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/local/40435.rb","EDB-ID":40435},

{"Exploit":"Linux Kernel 2.6.28 / 3.0 (DEC Alpha Linux) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/17391.c","EDB-ID":17391},

{"Exploit":"Linux Kernel < 2.6.36.2 (Ubuntu 10.04) - 'Half-Nelson.c' Econet Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/17787.c","EDB-ID":17787},

{"Exploit":"Linux Kernel 2.6.37-rc1 - 'serial\_multiport\_struct' Local Information Leak Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/18080.c","EDB-ID":18080},

{"Exploit":"Linux Kernel 2.6.39 < 3.2.2 (Gentoo / Ubuntu x86/x64) - 'Mempodipper.c' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/18411.c","EDB-ID":18411},

{"Exploit":"Slackware Linux 3.4 - liloconfig-color Temporary file","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19070.txt","EDB-ID":19070},

{"Exploit":"Slackware Linux 3.4 - makebootdisk Temporary file","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19071.txt","EDB-ID":19071},

{"Exploit":"Slackware Linux 3.4 - netconfig Temporary file","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19073.txt","EDB-ID":19073},

{"Exploit":"Slackware Linux 3.4 - pkgtool Temporary file","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19074.txt","EDB-ID":19074},

{"Exploit":"Slackware Linux 3.5 - Missing /etc/group Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19122.txt","EDB-ID":19122},

{"Exploit":"Caldera kdenetwork 1.1.1-1 / Caldera OpenLinux 1.3/2.2 / KDE KDE 1.1/1.1. / RedHat Linux 6.0 - K-Mail File Creation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19240.c","EDB-ID":19240},

{"Exploit":"S.u.S.E. Linux 5.2 - gnuplot Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19254.c","EDB-ID":19254},

{"Exploit":"RedHat Linux 5.2 i386/6.0 - No Logging","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19255.txt","EDB-ID":19255},

{"Exploit":"RedHat Linux 2.1 - abuse.console Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19279.sh","EDB-ID":19279},

{"Exploit":"RedHat Linux 5.1 xosview - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19281.c","EDB-ID":19281},

{"Exploit":"Slackware Linux 3.1 - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19283.c","EDB-ID":19283},

{"Exploit":"Slackware Linux 3.1 / 3.2 - color\_xterm Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19285.txt","EDB-ID":19285},

{"Exploit":"Slackware Linux 3.1 / 3.2 - color\_xterm Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19286.c","EDB-ID":19286},

{"Exploit":"Linux libc 5.3.12 / RedHat Linux 4.0 / Slackware Linux 3.1 - libc NLSPATH","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19302.c","EDB-ID":19302},

{"Exploit":"RedHat Linux 5.0 msgchk - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19305.c","EDB-ID":19305},

{"Exploit":"RedHat Linux 4.2 / SGI IRIX 6.3 / Solaris 2.6 mailx - Exploit (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19311.c","EDB-ID":19311},

{"Exploit":"RedHat Linux 4.2 / SGI IRIX 6.3 / Solaris 2.6 mailx - Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19312.c","EDB-ID":19312},

{"Exploit":"RedHat Linux 5.0/5.1/5.2 / Slackware Linux 3.5 - klogd Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19314.c","EDB-ID":19314},

{"Exploit":"RedHat Linux 5.0/5.1/5.2 / Slackware Linux 3.5 - klogd Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19315.c","EDB-ID":19315},

{"Exploit":"Linux libc 5.3.12/5.4 / RedHat Linux 4.0 - vsyslog() Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19360.c","EDB-ID":19360},

{"Exploit":"Linux Kernel 2.0.37 - Segment Limit Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19419.c","EDB-ID":19419},

{"Exploit":"RedHat Linux 6.0 / Slackware Linux 4.0 - Termcap tgetent() Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19464.c","EDB-ID":19464},

{"Exploit":"RedHat Linux 6.0 / Slackware Linux 4.0 - Termcap tgetent() Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19465.c","EDB-ID":19465},

{"Exploit":"RedHat Linux 4.2/5.2/6.0 / S.u.S.E. Linux 6.0/6.1 - Cron Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19469.c","EDB-ID":19469},

{"Exploit":"RedHat Linux 4.2/5.2/6.0 / S.u.S.E. Linux 6.0/6.1 - Cron Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19470.c","EDB-ID":19470},

{"Exploit":"Caldera OpenLinux 2.2 / Debian 2.1/2.2 / RedHat 6.0 - Vixie Cron MAILTO Sendmail","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19474.txt","EDB-ID":19474},

{"Exploit":"ISC INN 2.2 / RedHat Linux 6.0 - inews Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/local/19480.c","EDB-ID":19480},

{"Exploit":"S.u.S.E. Linux 6.2 sscw - HOME Environment Variable Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19508.sh","EDB-ID":19508},

{"Exploit":"Mandriva Linux Mandrake 6.0 / Gnome Libs 1.0.8 espeaker - Local Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19512.sh","EDB-ID":19512},

{"Exploit":"S.u.S.E. Linux 6.1/6.2 - cwdtools Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19565.sh","EDB-ID":19565},

{"Exploit":"FreeBSD 3.3/Linux Mandrake 7.0 - 'xsoldier' Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/freebsd/local/19676.c","EDB-ID":19676},

{"Exploit":"FreeBSD 3.3/Linux Mandrake 7.0 - 'xsoldier' Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19677.c","EDB-ID":19677},

{"Exploit":"IRIX 6.5 / Solaris 7.0 / Turbolinux 4.2 - 'uum' Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19582.c","EDB-ID":19582},

{"Exploit":"Turbolinux 3.5 b2 - 'canuum' Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19583.c","EDB-ID":19583},

{"Exploit":"Mandrake 6.x / RedHat 6.x / Turbolinux 3.5 b2/4.x/6.0.2 userhelper/PAM - Path Exploit (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19709.sh","EDB-ID":19709},

{"Exploit":"Mandrake 6.x / RedHat 6.x / Turbolinux 3.5 b2/4.x/6.0.2 userhelper/PAM - Path Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19710.c","EDB-ID":19710},

{"Exploit":"Corel Linux OS 1.0 - get\_it PATH","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19723.txt","EDB-ID":19723},

{"Exploit":"RedHat Linux 6.0 - Single User Mode Authentication","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19763.txt","EDB-ID":19763},

{"Exploit":"Corel Linux OS 1.0 - buildxconfig Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19764.txt","EDB-ID":19764},

{"Exploit":"Corel Linux OS 1.0 - setxconf Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19765.txt","EDB-ID":19765},

{"Exploit":"RedHat 4.x/5.x/6.x / RedHat man 1.5 / Turbolinux man 1.5 / Turbolinux 3.5/4.x man - Buffer Overrun (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19778.c","EDB-ID":19778},

{"Exploit":"RedHat 4.x/5.x/6.x / RedHat man 1.5 / Turbolinux man 1.5 / Turbolinux 3.5/4.x man - Buffer Overrun (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19779.c","EDB-ID":19779},

{"Exploit":"Corel Linux OS 1.0 - Denial of Serviceemu Distribution Configuration","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19787.txt","EDB-ID":19787},

{"Exploit":"Oracle8i Standard Edition 8.1.5 for Linux Installer - Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19794.txt","EDB-ID":19794},

{"Exploit":"Matt Kimball and Roger Wolff mtr 0.28/0.41 / Turbolinux 3.5 b2/4.2/4.4/6.0 - mtr Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/local/19796.c","EDB-ID":19796},

{"Exploit":"AT Computing atsar\_linux 1.4 - File Manipulation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19804.pl","EDB-ID":19804},

{"Exploit":"Halloween Linux 4.0 / RedHat Linux 6.1/6.2 - imwheel Exploit (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19811.c","EDB-ID":19811},

{"Exploit":"Halloween Linux 4.0 / RedHat Linux 6.1/6.2 - imwheel Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19812.c","EDB-ID":19812},

{"Exploit":"Halloween Linux 4.0 / S.u.S.E. Linux 6.0/6.1/6.2/6.3 - kreatecd Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19813.txt","EDB-ID":19813},

{"Exploit":"Bray Systems Linux Trustees 1.5 - Long Pathname","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19837.c","EDB-ID":19837},

{"Exploit":"S.u.S.E. Linux 6.x - Arbitrary File Deletion","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19867.txt","EDB-ID":19867},

{"Exploit":"S.u.S.E. Linux 6.3/6.4 Gnomelib - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19883.c","EDB-ID":19883},

{"Exploit":"RedHat Linux 6.0/6.1/6.2 - pam\_console Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19900.c","EDB-ID":19900},

{"Exploit":"Linux Kernel 2.4.4 < 2.4.37.4 / 2.6.0 < 2.6.30.4 - 'Sendpage' Privilege Escalation (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19933.rb","EDB-ID":19933},

{"Exploit":"S.u.S.E. 4.x/5.x/6.x/7.0 / Slackware 3.x/4.0 / Turbolinux 6 / OpenLinux 7.0 - fdmount Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19952.c","EDB-ID":19952},

{"Exploit":"S.u.S.E. 4.x/5.x/6.x/7.0 / Slackware 3.x/4.0 / Turbolinux 6 / OpenLinux 7.0 - fdmount Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19953.c","EDB-ID":19953},

{"Exploit":"S.u.S.E. 4.x/5.x/6.x/7.0 / Slackware 3.x/4.0 / Turbolinux 6 / OpenLinux 7.0 - fdmount Buffer Overflow (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19954.c","EDB-ID":19954},

{"Exploit":"Mandriva Linux Mandrake 7.0 - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19969.c","EDB-ID":19969},

{"Exploit":"Linux Kernel 2.2.x 2.4.0-test1 (SGI ProPack 1.2/1.3) - (Sendmail) Capabilities Privilege Escalation(1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20000.c","EDB-ID":20000},

{"Exploit":"Linux Kernel 2.2.x 2.4.0-test1 (SGI ProPack 1.2/1.3) - (Sendmail 8.10.1) Capabilities Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20001.sh","EDB-ID":20001},

{"Exploit":"Nvidia Linux Driver - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20201.c","EDB-ID":20201},

{"Exploit":"Linux modutils 2.3.9 - modprobe Arbitrary Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20402.sh","EDB-ID":20402},

{"Exploit":"Linux Kernel 2.2.x - Non-Readable File Ptrace Local Information Leak","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20458.txt","EDB-ID":20458},

{"Exploit":"Linux Kernel 2.2.x - sysctl() Memory Reading (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20626.c","EDB-ID":20626},

{"Exploit":"Linux Kernel 2.2.18 (RedHat 7.0/6.2 & 2.2.14 / 2.2.18 / 2.2.18ow4) - ptrace/execve Race Condition Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20720.c","EDB-ID":20720},

{"Exploit":"Linux Kernel 2.2.18 (RedHat 7.0/6.2 & 2.2.14 / 2.2.18 / 2.2.18ow4) - ptrace/execve Race Condition Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20721.c","EDB-ID":20721},

{"Exploit":"Linux 6.1/6.2/7.0/7.1 Man Page - Source Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20926.txt","EDB-ID":20926},

{"Exploit":"Linux Kernel 2.2 / 2.4 - procfs Stream redirection to Process Memory Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/20979.c","EDB-ID":20979},

{"Exploit":"Linux Kernel 2.2 / 2.4 - Ptrace/Setuid Exec Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21124.txt","EDB-ID":21124},

{"Exploit":"(Linux Kernel 2.4.17-8) User-Mode Linux - Memory Access Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21248.txt","EDB-ID":21248},

{"Exploit":"Century Software Term For Linux 6.27.869 - Command Line Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21302.c","EDB-ID":21302},

{"Exploit":"Linux Kernel 2.2.x / 2.3 / 2.4.x - d\_path() Path Truncation (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21353.c","EDB-ID":21353},

{"Exploit":"(Linux Kernel) Grsecurity Kernel Patch 1.9.4 - Memory Protection","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21458.txt","EDB-ID":21458},

{"Exploit":"ISDN4Linux 3.1 - IPPPD Device String SysLog Format String (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21700.c","EDB-ID":21700},

{"Exploit":"ISDN4Linux 3.1 - IPPPD Device String SysLog Format String (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21701.pl","EDB-ID":21701},

{"Exploit":"Linuxconf 1.1.x / 1.2.x - Local Environment Variable Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21761.c","EDB-ID":21761},

{"Exploit":"Linuxconf 1.1.x / 1.2.x - Local Environment Variable Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21762.c","EDB-ID":21762},

{"Exploit":"Linuxconf 1.1.x / 1.2.x - Local Environment Variable Buffer Overflow (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21763.txt","EDB-ID":21763},

{"Exploit":"Cobalt Linux 6.0 - RaQ Authenticate Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/21790.sh","EDB-ID":21790},

{"Exploit":"Linux Kernel UDEV < 1.4.1 - Netlink Privilege Escalation (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/21848.rb","EDB-ID":21848},

{"Exploit":"Linux Kernel 2.2.x / 2.4.x - Privileged Process Hijacking Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/22362.c","EDB-ID":22362},

{"Exploit":"Linux Kernel 2.2.x / 2.4.x - Privileged Process Hijacking Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/22363.c","EDB-ID":22363},

{"Exploit":"Linux Kernel 2.2.x / 2.4.x - I/O System Call File Existence","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/22458.c","EDB-ID":22458},

{"Exploit":"Linux-ATM LES 2.4 - Command Line Argument Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/22540.c","EDB-ID":22540},

{"Exploit":"Linux PAM 0.77 - Pam\_Wheel Module getlogin() 'Username' Spoofing Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/22781.txt","EDB-ID":22781},

{"Exploit":"Linux Kernel 2.2.x / 2.4.x - /proc Filesystem Potential Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/22813.c","EDB-ID":22813},

{"Exploit":"Linux Kernel 2.4 - SUID execve() System Call Race Condition Executable File Read (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/22840.c","EDB-ID":22840},

{"Exploit":"MySQL (Linux) - Database Privilege Elevation Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/23077.pl","EDB-ID":23077},

{"Exploit":"RealOne Player for Linux 2.2 Alpha - Insecure Configuration File Permission Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/23126.c","EDB-ID":23126},

{"Exploit":"SuSE Linux Professional 8.2 - SuSEWM Configuration File Insecure Temporary File","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/23223.c","EDB-ID":23223},

{"Exploit":"Linux VServer Project 1.2x - CHRoot Breakout","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/23658.c","EDB-ID":23658},

{"Exploit":"(Linux Kernel 2.6) Samba 2.2.8 (Debian / Mandrake) - Share Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/23674.txt","EDB-ID":23674},

{"Exploit":"Linux Kernel 2.5.x / 2.6.x - CPUFreq Proc Handler Integer Handling Memory Read","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/24043.c","EDB-ID":24043},

{"Exploit":"Linux Kernel 2.6.32-5 (Debian 6.0.5) - /dev/ptmx Key Stroke Timing Local Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/24459.sh","EDB-ID":24459},

{"Exploit":"Linux Kernel < 3.3.x < 3.7.x (Arch Linux x86-64) - 'sock\_diag\_handlers[]' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/24555.c","EDB-ID":24555},

{"Exploit":"Linux Kernel 3.7.10 (Ubuntu 12.10 x64) - 'sock\_diag\_handlers' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/24746.c","EDB-ID":24746},

{"Exploit":"Linux Kernel 2.6.x - 'SYS\_EPoll\_Wait' Local Integer Overflow Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/25202.c","EDB-ID":25202},

{"Exploit":"Linux Kernel 2.4.x / 2.6.x - BlueTooth Signed Buffer Index Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/25288.c","EDB-ID":25288},

{"Exploit":"Linux Kernel 2.4.30 / 2.6.11.5 - BlueTooth 'bluez\_sock\_create' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/25289.c","EDB-ID":25289},

{"Exploit":"Linux Kernel 2.6.32 < 3.x.x (CentOS) - 'PERF\_EVENTS' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/25444.c","EDB-ID":25444},

{"Exploit":"Linux Kernel < 3.8.x - open-time Capability file\_ns\_capable() Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/25450.c","EDB-ID":25450},

{"Exploit":"Linux Kernel 2.6.x - Cryptoloop Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/25707.txt","EDB-ID":25707},

{"Exploit":"Linux Kernel < 3.8.9 (x86-64) - 'perf\_swevent\_init' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/26131.c","EDB-ID":26131},

{"Exploit":"Linux Kernel 2.6 - Console Keymap Local Command Injection (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/26353.txt","EDB-ID":26353},

{"Exploit":"Linux Kernel 3.7.6 (RedHat x86/x64) - 'MSR' Driver Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/27297.c","EDB-ID":27297},

{"Exploit":"Linux Kernel 2.4.x/2.5.x/2.6.x - Sockaddr\_In.Sin\_Zero Kernel Memory Disclosure Vulnerabilities","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/27461.c","EDB-ID":27461},

{"Exploit":"Linux Kernel 2.6.x - SMBFS CHRoot Security Restriction Bypass","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/27766.txt","EDB-ID":27766},

{"Exploit":"Linux Kernel 2.6.x - CIFS CHRoot Security Restriction Bypass","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/27769.txt","EDB-ID":27769},

{"Exploit":"Linux-HA Heartbeat 1.2.3/2.0.x - Insecure Default Permissions on Shared Memory","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/28287.c","EDB-ID":28287},

{"Exploit":"Linux Kernel 2.6.17 - 'Sys\_Tee' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/29714.txt","EDB-ID":29714},

{"Exploit":"Linux Kernel 2.6.x - Ptrace Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/30604.c","EDB-ID":30604},

{"Exploit":"Linux Kernel 2.6.x - ALSA snd-page-alloc Local Proc File Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/30605.c","EDB-ID":30605},

{"Exploit":"Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG\_X86\_X32' Arbitrary Write Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/31346.c","EDB-ID":31346},

{"Exploit":"Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10) - 'CONFIG\_X86\_X32=y' Privilege Escalation (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/local/31347.c","EDB-ID":31347},

{"Exploit":"Linux Kernel < 3.4.5 (Android 4.2.2 / 4.4 ARM) - Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/local/31574.c","EDB-ID":31574},

{"Exploit":"Systrace 1.x (x64) - Aware Linux Kernel Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/32751.c","EDB-ID":32751},

{"Exploit":"Linux Kernel 2.6.x - 'sock.c' SO\_BSDCOMPAT Option Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/32805.c","EDB-ID":32805},

{"Exploit":"Linux Kernel 2.6.x - 'seccomp' System Call Security Bypass","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/32829.c","EDB-ID":32829},

{"Exploit":"Linux Kernel 2.6.0 < 2.6.31 - 'pipe.c' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/33321.c","EDB-ID":33321},

{"Exploit":"Linux Kernel 2.6.x - 'pipe.c' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/33322.c","EDB-ID":33322},

{"Exploit":"Linux Kernel 3.3 < 3.8 (Ubuntu / Fedora 18) - 'sock\_diag\_handlers()' Privilege Escalation (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/33336.c","EDB-ID":33336},

{"Exploit":"Linux Kernel 2.6.x - Ext4 'move extents' ioctl Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/33395.txt","EDB-ID":33395},

{"Exploit":"Linux Kernel 3.14-rc1 < 3.15-rc4 (x64) - Raw Mode PTY Local Echo Race Condition Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/33516.c","EDB-ID":33516},

{"Exploit":"Linux Kernel 3.2.0-23 / 3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf\_swevent\_init' Privilege Escalation (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/33589.c","EDB-ID":33589},

{"Exploit":"Linux Kernel < 2.6.28 - 'fasync\_helper()' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/33523.c","EDB-ID":33523},

{"Exploit":"Linux Kernel 3.13 - (SGID) Privilege Escalation (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/33824.c","EDB-ID":33824},

{"Exploit":"Linux Kernel 2.6.x - Btrfs Cloned File Security Bypass","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/34001.c","EDB-ID":34001},

{"Exploit":"Linux Kernel < 3.2.0-23 (Ubuntu 12.04 x64) - 'ptrace/sysret' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/34134.c","EDB-ID":34134},

{"Exploit":"Linux Kernel < 3.16.1 - 'Remount FUSE' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/34923.c","EDB-ID":34923},

{"Exploit":"Linux Kernel 2.6.x - 'net/core/filter.c' Local Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/34987.c","EDB-ID":34987},

{"Exploit":"Linux PolicyKit - Race Condition Privilege Escalation (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/35021.rb","EDB-ID":35021},

{"Exploit":"Linux Kernel 2.6.39 < 3.2.2 (x86/x64) - 'Mempodipper.c' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/35161.c","EDB-ID":35161},

{"Exploit":"Linux Kernel 3.14.5 (RHEL / CentOS 7) - 'libfutex' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/35370.c","EDB-ID":35370},

{"Exploit":"Offset2lib - Bypassing Full ASLR On 64 bit Linux","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/35472.txt","EDB-ID":35472},

{"Exploit":"Linux Kernel 3.0.4 - '/proc/interrupts' Password Length Local Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/36294.c","EDB-ID":36294},

{"Exploit":"Linux Kernel (x86-64) - Rowhammer Privilege Escalation (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/36310.txt","EDB-ID":36310},

{"Exploit":"Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/37292.c","EDB-ID":37292},

{"Exploit":"Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation (Access /etc/shadow)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/37293.txt","EDB-ID":37293},

{"Exploit":"Linux Kernel 2.6.x - 'rds\_recvmsg()' Function Local Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/37543.c","EDB-ID":37543},

{"Exploit":"Linux espfix64 - (Nested NMIs Interrupting) Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/37722.c","EDB-ID":37722},

{"Exploit":"Linux (x86) - Memory Sinkhole Privilege Escalation (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/local/37724.asm","EDB-ID":37724},

{"Exploit":"Linux Kernel 3.2.x - 'uname()' System Call Local Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/37937.c","EDB-ID":37937},

{"Exploit":"Linux Kernel 3.0 < 3.3.5 - 'CLONE\_NEWUSER|CLONE\_FS' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/38390.c","EDB-ID":38390},

{"Exploit":"Linux 3.17 - noexec File Security Bypass (Python ctypes and memfd\_create)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/38473.py","EDB-ID":38473},

{"Exploit":"Linux Kernel 3.3.5 - 'b43' Wireless Driver Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/38559.txt","EDB-ID":38559},

{"Exploit":"Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/39166.c","EDB-ID":39166},

{"Exploit":"Linux Kernel 3.3.5 - '/drivers/media/media-device.c' Local Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/39214.c","EDB-ID":39214},

{"Exploit":"Linux Kernel 4.3.3 - 'overlayfs' Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/39230.c","EDB-ID":39230},

{"Exploit":"Linux Kernel 4.4.1 - REFCOUNT Overflow/Use-After-Free in Keyrings Privilege Escalation (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/39277.c","EDB-ID":39277},

{"Exploit":"Linux Kernel 4.4.1 - REFCOUNT Overflow/Use-After-Free in Keyrings Privilege Escalation (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40003.c","EDB-ID":40003},

{"Exploit":"Deepin Linux 15 - 'lastore-daemon' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/39433.py","EDB-ID":39433},

{"Exploit":"Linux Kernel (Ubuntu 14.04.3) - 'perf\_event\_open()' Can Race with execve() (Access /etc/shadow)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/39771.txt","EDB-ID":39771},

{"Exploit":"Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF\_PROG\_LOAD) Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/39772.txt","EDB-ID":39772},

{"Exploit":"Linux - ecryptfs and /proc/$pid/environ Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/39992.txt","EDB-ID":39992},

{"Exploit":"Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter target\_offset Out-of-Bounds Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/40049.c","EDB-ID":40049},

{"Exploit":"Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T\_SO\_SET\_REPLACE' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40489.txt","EDB-ID":40489},

{"Exploit":"Linux Kernel 3.13.1 - 'Recvmmsg' Privilege Escalation (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40503.rb","EDB-ID":40503},

{"Exploit":"Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (PoC) (Write Access)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40611.c","EDB-ID":40611},

{"Exploit":"Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW' /proc/self/mem Race Condition Privilege Escalation (SUID)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40616.c","EDB-ID":40616},

{"Exploit":"Linux Kernel (Ubuntu / Fedora / RedHat) - 'Overlayfs' Privilege Escalation (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40688.rb","EDB-ID":40688},

{"Exploit":"Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' PTRACE\_POKEDATA Race Condition (PoC) (Write Access)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40838.c","EDB-ID":40838},

{"Exploit":"Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Privilege Escalation (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40759.rb","EDB-ID":40759},

{"Exploit":"Linux Kernel 2.6.18 - 'move\_pages()' Information Leak","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40810.c","EDB-ID":40810},

{"Exploit":"Linux Kernel 2.6.32-rc1 (x86-64) - Register Leak","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/40811.c","EDB-ID":40811},

{"Exploit":"Linux Kernel 2.6.10 < 2.6.31.5 - 'pipe.c' Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40812.c","EDB-ID":40812},

{"Exploit":"Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' PTRACE\_POKEDATA Race Condition Privilege Escalation (/etc/passwd)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40839.c","EDB-ID":40839},

{"Exploit":"Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition Privilege Escalation (/etc/passwd)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/40847.cpp","EDB-ID":40847},

{"Exploit":"Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF\_PACKET' Race Condition Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/local/40871.c","EDB-ID":40871},

{"Exploit":"Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/41458.c","EDB-ID":41458},

{"Exploit":"Linux Kernel 2.6.32 (Ubuntu 10.04) - /proc Handling SUID Privilege Escalation","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/41770.txt","EDB-ID":41770},

{"Exploit":"Linux eXtremail 1.5.x - Remote Format Strings Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/49.c","EDB-ID":49},

{"Exploit":"Real Server 7/8/9 (Windows / Linux) - Remote Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/86.c","EDB-ID":86},

{"Exploit":"Linux pam\_lib\_smb < 1.1.6 - /bin/login Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/89.c","EDB-ID":89},

{"Exploit":"PHF (Linux/x86) - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/cgi/remote/211.c","EDB-ID":211},

{"Exploit":"Linux Kernel 2.2 - TCP/IP Weakness Spoof IP Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/237.c","EDB-ID":237},

{"Exploit":"BeroFTPD 1.3.4(1) (Linux x86) - Remote Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/remote/269.c","EDB-ID":269},

{"Exploit":"CVS (Linux/FreeBSD) - Remote Entry Line Heap Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/300.c","EDB-ID":300},

{"Exploit":"Linux imapd - Remote Overflow File Retrieve Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/340.c","EDB-ID":340},

{"Exploit":"SHOUTcast DNAS/Linux 1.9.4 - Format String Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/712.c","EDB-ID":712},

{"Exploit":"MSN Messenger (Linux) - '.png' Image Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/windows/remote/804.c","EDB-ID":804},

{"Exploit":"Medal of Honor Spearhead (Linux) - Server Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/826.c","EDB-ID":826},

{"Exploit":"Ethereal 0.10.9 (Linux) - '3G-A11' Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/878.c","EDB-ID":878},

{"Exploit":"dSMTP Mail Server 3.1b (Linux) - Format String Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/981.c","EDB-ID":981},

{"Exploit":"RealPlayer/Helix Player (Linux) - Remote Format String","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/1232.c","EDB-ID":1232},

{"Exploit":"Veritas NetBackup 6.0 (Linux) - (bpjava-msvc) Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/1263.pl","EDB-ID":1263},

{"Exploit":"linux-ftpd-ssl 0.17 - 'MKD'/'CWD' Remote Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/1295.c","EDB-ID":1295},

{"Exploit":"Mozilla Firefox 1.5 (Linux) - location.QueryInterface() Code Execution (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/1474.pm","EDB-ID":1474},

{"Exploit":"Snort 2.6.1 (Linux) - DCE/RPC Preprocessor Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/3609.py","EDB-ID":3609},

{"Exploit":"dproxy-nexgen (Linux x86) - Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/remote/3615.c","EDB-ID":3615},

{"Exploit":"3proxy 0.5.3g (Linux) - proxy.c logurl() Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/3821.c","EDB-ID":3821},

{"Exploit":"Debian OpenSSH - Authenticated Remote SELinux Privilege Elevation Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/6094.txt","EDB-ID":6094},

{"Exploit":"Linux Kernel 2.6.20 / 2.6.24 / 2.6.27\_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora Core 10 / OpenSuse 11.1) - SCTP FWD Memory Corruption Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/8556.c","EDB-ID":8556},

{"Exploit":"Skype for Linux 2.1 Beta - Multiple Strange Behaviour","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/10980.txt","EDB-ID":10980},

{"Exploit":"McAfee LinuxShield 1.5.1 - Local/Remote File Inclusion (Remote Code Execution)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/14818.pl","EDB-ID":14818},

{"Exploit":"Unreal Tournament 2004 (Linux) - 'secure' Overflow (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/16848.rb","EDB-ID":16848},

{"Exploit":"MySQL yaSSL (Linux) - SSL Hello Message Buffer Overflow (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/16849.rb","EDB-ID":16849},

{"Exploit":"ProFTPd 1.3.2rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/16851.rb","EDB-ID":16851},

{"Exploit":"ProFTPd 1.2 < 1.3.0 (Linux) - sreplace Buffer Overflow (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/16852.rb","EDB-ID":16852},

{"Exploit":"PeerCast 0.1216 (Linux) - URL Handling Buffer Overflow (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/16855.rb","EDB-ID":16855},

{"Exploit":"Samba 3.0.24 (Linux) - 'lsa\_io\_trans\_names' Heap Overflow (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/16859.rb","EDB-ID":16859},

{"Exploit":"Samba 3.3.12 (Linux x86) - 'chain\_reply' Memory Corruption (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/remote/16860.rb","EDB-ID":16860},

{"Exploit":"Samba 2.2.8 (Linux x86) - 'trans2open' Overflow (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/remote/16861.rb","EDB-ID":16861},

{"Exploit":"HP Data Protector (Linux) - Remote Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/17648.sh","EDB-ID":17648},

{"Exploit":"Linux BSD-derived Telnet Service Encryption Key ID - Buffer Overflow (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/18368.rb","EDB-ID":18368},

{"Exploit":"RedHat Linux 5.1 & Caldera OpenLinux Standard 1.2 - Mountd","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/19096.c","EDB-ID":19096},

{"Exploit":"SGI Advanced Linux Environment 3.0 / SGI IRIX 6.5.4 / SGI UNICOS 10.0 6 - arrayd.auth Default Configuration","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/19426.c","EDB-ID":19426},

{"Exploit":"Linux Kernel 2.0.30/2.0.35/2.0.36/2.0.37 - Blind TCP Spoofing","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/19458.c","EDB-ID":19458},

{"Exploit":"BSD/OS 3.1/4.0.1 / FreeBSD 3.0/3.1/3.2 / RedHat Linux 6.0 - amd Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/remote/19478.c","EDB-ID":19478},

{"Exploit":"BSD/OS 3.1/4.0.1 / FreeBSD 3.0/3.1/3.2 / RedHat Linux 6.0 - amd Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/remote/19479.c","EDB-ID":19479},

{"Exploit":"Linux Kernel 2.2 - Predictable TCP Initial Sequence Number","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/19522.txt","EDB-ID":19522},

{"Exploit":"Caldera OpenLinux 2.3 - rpm\_query CGI","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/cgi/remote/19795.txt","EDB-ID":19795},

{"Exploit":"S.u.S.E. Linux 6.3/6.4 - Installed Package Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20236.txt","EDB-ID":20236},

{"Exploit":"TalentSoft Web+ Application Server (Linux) 4.6 - Example Script File Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20246.txt","EDB-ID":20246},

{"Exploit":"Trlinux Postaci Webmail 1.1.3 - Password Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/20450.txt","EDB-ID":20450},

{"Exploit":"IBM DB2 - Universal Database for Linux 6.1/Windows NT 6.1 Known Default Password","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/20472.txt","EDB-ID":20472},

{"Exploit":"Linuxconf 1.1.6 r10 - Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20619.c","EDB-ID":20619},

{"Exploit":"Linux Kernel 2.4 - IPTables FTP Stateful Inspection Arbitrary Filter Rule Insertion","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20765.pl","EDB-ID":20765},

{"Exploit":"SGI IRIX 3/4/5/6 / OpenLinux 1.0/1.1 - routed traceon Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/irix/remote/20805.c","EDB-ID":20805},

{"Exploit":"RedHat Linux 7.0 Apache - Remote 'Username' Enumeration","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/21112.php","EDB-ID":21112},

{"Exploit":"HP SiteScope (Linux/Windows) - Remote Code Execution (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/21137.rb","EDB-ID":21137},

{"Exploit":"Linux Kernel 2.0.x/2.2.x/2.4.x (FreeBSD 4.x) - Network Device Driver Frame Padding Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/bsd/remote/22131.pl","EDB-ID":22131},

{"Exploit":"Antologic Antolinux 1.0 - Administrative Interface NDCR Parameter Remote Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/23604.txt","EDB-ID":23604},

{"Exploit":"Astaro Security Linux 6.0 01 - HTTP CONNECT Unauthorized Access","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/26198.txt","EDB-ID":26198},

{"Exploit":"RedHat CloudForms Management Engine 5.1 - agent/linuxpkgs Directory Traversal (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/30469.rb","EDB-ID":30469},

{"Exploit":"Nginx 1.4.0 (x64) (Generic Linux) - Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/remote/32277.txt","EDB-ID":32277},

{"Exploit":"XAMPP Linux 1.6 - ming.php text Parameter Cross-Site Scripting","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/32165.txt","EDB-ID":32165},

{"Exploit":"XAMPP Linux 1.6 - iart.php text Parameter Cross-Site Scripting","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/32166.txt","EDB-ID":32166},

{"Exploit":"Astaro Security Linux 5 - 'index.fpl' Cross-Site Scripting","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/33783.txt","EDB-ID":33783},

{"Exploit":"Linux/MIPS Kernel 2.6.36 - 'NetUSB' Remote Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/38454.py","EDB-ID":38454},

{"Exploit":"Linux Kernel 3.0.5 - 'ath9k\_htc\_set\_bssid\_mask()' Function Information Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/38826.py","EDB-ID":38826},

{"Exploit":"Xdh / LinuxNet Perlbot / fBot IRC Bot - Remote Code Execution (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/38974.rb","EDB-ID":38974},

{"Exploit":"McAfee Virus Scan Enterprise for Linux 1.9.2 < 2.0.2 - Remote Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/40911.py","EDB-ID":40911},

{"Exploit":"Linux/ARM - setuid(0) & execve(\_/bin/sh\_\_\_/bin/sh\_\_0) Shellcode (38 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/14113.txt","EDB-ID":14113},

{"Exploit":"Linux/x86 - execve Null Free Shellcode (Generator)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/generator/shellcode/13281.c","EDB-ID":13281},

{"Exploit":"Linux/x86 - Portbind Payload Shellcode (Generator)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/generator/shellcode/13282.php","EDB-ID":13282},

{"Exploit":"Linux/x86 - cmd Null Free Shellcode (Generator)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/generator/shellcode/13285.c","EDB-ID":13285},

{"Exploit":"Linux/x86-64 - flush iptables rules Shellcode (84 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/13296.c","EDB-ID":13296},

{"Exploit":"Linux/x86-64 - connect-back semi-stealth Shellcode (88+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/13297.c","EDB-ID":13297},

{"Exploit":"Linux/MIPS (Linksys WRT54G/GL) - 4919 port bind Shellcode (276 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/13298.c","EDB-ID":13298},

{"Exploit":"Linux/MIPS (Linksys WRT54G/GL) - execve Shellcode (60 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/13299.c","EDB-ID":13299},

{"Exploit":"Linux/MIPS - execve /bin/sh Shellcode (56 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/13300.c","EDB-ID":13300},

{"Exploit":"Linux/PPC - execve /bin/sh Shellcode (60 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_ppc/shellcode/13301.c","EDB-ID":13301},

{"Exploit":"Linux/PPC - read & exec Shellcode (32 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_ppc/shellcode/13302.c","EDB-ID":13302},

{"Exploit":"Linux/PPC - connect back (192.168.1.1:31337) execve /bin/sh Shellcode (240 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_ppc/shellcode/13303.c","EDB-ID":13303},

{"Exploit":"Linux/PPC - execve /bin/sh Shellcode (112 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_ppc/shellcode/13304.c","EDB-ID":13304},

{"Exploit":"Linux/SPARC - connect back (192.168.100.1:2313) Shellcode (216 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_sparc/shellcode/13305.c","EDB-ID":13305},

{"Exploit":"Linux/SPARC - portbind port 8975 Shellcode (284 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_sparc/shellcode/13306.c","EDB-ID":13306},

{"Exploit":"Linux/x86 - Self-modifying Shellcode for IDS evasion (64 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13307.c","EDB-ID":13307},

{"Exploit":"Linux/x86 - Forks a HTTP Server on port 8800/TCP Shellcode (166 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13308.c","EDB-ID":13308},

{"Exploit":"Linux/x86 - Listens for Shellcode on 5555/TCP and jumps to it (83 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13309.asm","EDB-ID":13309},

{"Exploit":"Linux/x86 - Polymorphic Shellcode disable Network Card (75 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13310.c","EDB-ID":13310},

{"Exploit":"Linux/x86 - killall5 polymorphic Shellcode (61 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13311.c","EDB-ID":13311},

{"Exploit":"Linux/x86 - /bin/sh polymorphic Shellcode (48 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13312.c","EDB-ID":13312},

{"Exploit":"Linux/x86 - 4444 Port Binding Shellcode (xor-encoded) (152 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13313.c","EDB-ID":13313},

{"Exploit":"Linux/x86 - reboot() polymorphic Shellcode (57 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13314.c","EDB-ID":13314},

{"Exploit":"Linux/x86 - Polymorphic chmod(\_/etc/shadow\_\_666) Shellcode (54 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13315.c","EDB-ID":13315},

{"Exploit":"Linux/x86 - setreuid(geteuid()\_geteuid())\_execve(\_/bin/sh\_\_0\_0) Shellcode (34 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13316.c","EDB-ID":13316},

{"Exploit":"Linux/x86 - bindport 8000 & execve iptables -F Shellcode (176 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13317.s","EDB-ID":13317},

{"Exploit":"Linux/x86 - bindport 8000 & add user with root access Shellcode (225+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13318.s","EDB-ID":13318},

{"Exploit":"Linux/x86 - 8000 Bind Port ASM Code Linux Shellcode (179 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13319.s","EDB-ID":13319},

{"Exploit":"Linux/x86-64 - setuid(0) + execve(/bin/sh) Shellcode (49 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13320.c","EDB-ID":13320},

{"Exploit":"Linux/x86 - Serial port shell binding & busybox Launching Shellcode (82 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13321.c","EDB-ID":13321},

{"Exploit":"Linux/x86 - File unlinker Shellcode (18+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13322.c","EDB-ID":13322},

{"Exploit":"Linux/x86 - Perl script execution Shellcode (99+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13323.c","EDB-ID":13323},

{"Exploit":"Linux/x86 - file reader Shellcode (65+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13324.c","EDB-ID":13324},

{"Exploit":"Linux/x86 - chmod(\_/etc/shadow\_\_666) & exit(0) Shellcode (30 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13325.c","EDB-ID":13325},

{"Exploit":"Linux/x86 - killall5 Shellcode (34 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13326.c","EDB-ID":13326},

{"Exploit":"Linux/x86 - PUSH reboot() Shellcode (30 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13327.c","EDB-ID":13327},

{"Exploit":"Linux/x86 - Shellcode obfuscator","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13328.c","EDB-ID":13328},

{"Exploit":"Linux/x86 - connect-back port UDP/54321 live packet capture Shellcode (151 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13329.c","EDB-ID":13329},

{"Exploit":"Linux/x86 - append rsa key to /root/.ssh/authorized\_keys2 Shellcode (295 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13330.c","EDB-ID":13330},

{"Exploit":"Linux/x86 - Edit /etc/sudoers (ALL ALL=(ALL) NOPASSWD: ALL) for full access Shellcode (86 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13331.c","EDB-ID":13331},

{"Exploit":"Linux/x86 - Ho' Detector - Promiscuous mode detector Shellcode (56 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13332.c","EDB-ID":13332},

{"Exploit":"Linux/x86 - setuid(0) & execve(/bin/sh\_0\_0) Shellcode (28 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13333.txt","EDB-ID":13333},

{"Exploit":"Linux/x86 - setresuid(0\_0\_0) /bin/sh Shellcode (35 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13334.txt","EDB-ID":13334},

{"Exploit":"Linux/x86 - iopl(3); asm(cli); while(1){} Shellcode (12 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13335.c","EDB-ID":13335},

{"Exploit":"Linux/x86 - system-beep Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13336.c","EDB-ID":13336},

{"Exploit":"Linux/x86 - Connect back (140.115.53.35:9999)\_ download a file (cb) and execute Shellcode (149 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13337.c","EDB-ID":13337},

{"Exploit":"Linux/x86 - setreuid(geteuid\_ geteuid) + execve(/bin/sh) Shellcode (39 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13338.c","EDB-ID":13338},

{"Exploit":"Linux/x86 - Connect Back Port 8192.send.exit /etc/shadow Shellcode (155 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13339.asm","EDB-ID":13339},

{"Exploit":"Linux/x86 - writes a php connectback shell (/var/www/cb.php) to the filesystem Shellcode (508 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13340.c","EDB-ID":13340},

{"Exploit":"Linux/x86 - rm -rf / attempts to block the process from being stopped Shellcode (132 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13341.c","EDB-ID":13341},

{"Exploit":"Linux/x86 - setuid(0) . setgid(0) . aslr\_off Shellcode (79 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13342.c","EDB-ID":13342},

{"Exploit":"Linux/x86 - raw-socket ICMP/checksum shell Shellcode (235 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13343.asm","EDB-ID":13343},

{"Exploit":"Linux/x86 - /sbin/iptables -F Shellcode (40 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13344.c","EDB-ID":13344},

{"Exploit":"Linux/x86 - kill all processes Shellcode (11 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13345.c","EDB-ID":13345},

{"Exploit":"Linux/x86 - execve read Shellcode (92 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13346.s","EDB-ID":13346},

{"Exploit":"Linux/x86 - /sbin/ipchains -F Shellcode (40 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13347.c","EDB-ID":13347},

{"Exploit":"Linux/x86 - set system time to 0 and exit Shellcode (12 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13348.c","EDB-ID":13348},

{"Exploit":"Linux/x86 - Add root user 'r00t' with no password to /etc/passwd Shellcode (69 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13349.c","EDB-ID":13349},

{"Exploit":"Linux/x86 - chmod 0666 /etc/shadow Shellcode (36 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13350.c","EDB-ID":13350},

{"Exploit":"Linux/x86 - forkbomb Shellcode (7 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13351.c","EDB-ID":13351},

{"Exploit":"Linux/x86 - execve(rm -rf /) Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13352.c","EDB-ID":13352},

{"Exploit":"Linux/x86 - setuid(0) + execve(/bin/sh) Shellcode (28 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13353.c","EDB-ID":13353},

{"Exploit":"Linux/x86 - execve(/bin/sh) Shellcode (22 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13354.c","EDB-ID":13354},

{"Exploit":"Linux/x86 - HTTP/1.x GET\_ Downloads and execve() Shellcode (111+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13355.c","EDB-ID":13355},

{"Exploit":"Linux/x86 - executes command after setreuid Shellcode (49+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13356.c","EDB-ID":13356},

{"Exploit":"Linux/x86 - stdin re-open and /bin/sh exec Shellcode (39 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13357.c","EDB-ID":13357},

{"Exploit":"Linux/x86 - re-use of /bin/sh string in .rodata Shellcode (16 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13358.c","EDB-ID":13358},

{"Exploit":"Linux/x86 - setuid(0) and /bin/sh execve() Shellcode (30 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13359.c","EDB-ID":13359},

{"Exploit":"Linux/x86 - setuid/portbind (Port 31337) Shellcode (96 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13360.c","EDB-ID":13360},

{"Exploit":"Linux/x86 - portbind (2707) Shellcode (84 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13361.c","EDB-ID":13361},

{"Exploit":"Linux/x86 - execve() Diassembly Obfuscation Shellcode (32 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13362.c","EDB-ID":13362},

{"Exploit":"Linux/x86 - SET\_PORT() portbind 31337/TCP Shellcode (100 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13363.c","EDB-ID":13363},

{"Exploit":"Linux/x86 - SET\_IP() Connectback (192.168.13.22:31337) Shellcode (82 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13364.c","EDB-ID":13364},

{"Exploit":"Linux/x86 - execve(/bin/sh) Shellcode (24 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13365.c","EDB-ID":13365},

{"Exploit":"Linux/x86 - xor-encoded Connect Back (127.0.0.1:80) Shellcode (371 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13366.txt","EDB-ID":13366},

{"Exploit":"Linux/x86 - execve(/bin/sh) + ZIP Header Shellcode (28 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13367.c","EDB-ID":13367},

{"Exploit":"Linux/x86 - execve(/bin/sh) + RTF Header Shellcode (30 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13368.c","EDB-ID":13368},

{"Exploit":"Linux/x86 - execve(/bin/sh) + RIFF Header Shellcode (28 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13369.c","EDB-ID":13369},

{"Exploit":"Linux/x86 - execve(/bin/sh) + Bitmap Header Shellcode (27 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13370.c","EDB-ID":13370},

{"Exploit":"Linux/x86 - /tmp/swr to SWAP restore Shellcode (109 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13371.c","EDB-ID":13371},

{"Exploit":"Linux/x86 - SWAP store from /tmp/sws Shellcode (99 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13372.c","EDB-ID":13372},

{"Exploit":"Linux/x86 - Password Authentication portbind (64713) Shellcode (166 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13373.c","EDB-ID":13373},

{"Exploit":"Linux/x86 - portbind (port 64713) Shellcode (86 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13374.c","EDB-ID":13374},

{"Exploit":"Linux/x86 - execve(\_/bin/sh\_\_ [\_/bin/sh\_\_ NULL]) Shellcode (25 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13375.c","EDB-ID":13375},

{"Exploit":"Linux/x86 - execve(\_/bin/sh\_\_ [\_/bin/sh\_\_ NULL]) Shellcode (23 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13376.c","EDB-ID":13376},

{"Exploit":"Linux/x86 - setuid(0) + execve(\_/bin/sh\_\_ [\_/bin/sh\_\_ NULL]) Shellcode (31 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13377.c","EDB-ID":13377},

{"Exploit":"Linux/x86 - setuid(0)\_setgid(0) execve(/bin/sh\_ [/bin/sh\_ NULL]) Shellcode (37 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13378.c","EDB-ID":13378},

{"Exploit":"Linux/x86 - setreuid(0\_0) execve(\_/bin/sh\_\_ [\_/bin/sh\_\_ NULL]) Shellcode (33 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13379.c","EDB-ID":13379},

{"Exploit":"Linux/x86 - HTTP/1.x GET\_ Downloads and JMP Shellcode (68+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13380.c","EDB-ID":13380},

{"Exploit":"Linux/x86 - TCP Proxy Shellcode (236 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13381.c","EDB-ID":13381},

{"Exploit":"Linux/x86 - execve /bin/sh anti-ids Shellcode (40 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13382.c","EDB-ID":13382},

{"Exploit":"Linux/x86 - execve /bin/sh xored for Intel x86 CPUID Shellcode (41 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13383.c","EDB-ID":13383},

{"Exploit":"Linux/x86 - execve /bin/sh Shellcode (encoded by +1) (39 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13384.c","EDB-ID":13384},

{"Exploit":"Linux/x86 - Add User 'xtz' without Password to /etc/passwd Shellcode (59 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13385.c","EDB-ID":13385},

{"Exploit":"Linux/x86 - anti-debug trick (INT 3h trap) + execve /bin/sh Shellcode (39 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13386.c","EDB-ID":13386},

{"Exploit":"Linux/x86 - Bind /bin/sh to 31337/TCP Shellcode (80 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13387.c","EDB-ID":13387},

{"Exploit":"Linux/x86 - Bind /bin/sh to 31337/TCP + fork() Shellcode (98 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13388.c","EDB-ID":13388},

{"Exploit":"Linux/x86 - 24/7 open cd-rom loop (follows /dev/cdrom symlink) Shellcode (39 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13389.c","EDB-ID":13389},

{"Exploit":"Linux/x86 - eject cd-rom (follows /dev/cdrom symlink) + exit() Shellcode (40 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13390.c","EDB-ID":13390},

{"Exploit":"Linux/x86 - eject/close cd-rom loop (follows /dev/cdrom symlink) Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13391.c","EDB-ID":13391},

{"Exploit":"Linux/x86 - chmod(/etc/shadow\_ 0666) + exit() Shellcode (32 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13392.c","EDB-ID":13392},

{"Exploit":"Linux/x86 - Connect-back Shellcode 127.0.0.1:31337/TCP (74 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13393.c","EDB-ID":13393},

{"Exploit":"Linux/x86 - normal exit with random (so to speak) return value Shellcode (5 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13394.c","EDB-ID":13394},

{"Exploit":"Linux/x86 - getppid() + execve(/proc/pid/exe) Shellcode (51 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13395.c","EDB-ID":13395},

{"Exploit":"Linux/x86 - Quick (yet conditional\_ eax != 0 and edx == 0) exit Shellcode (4 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13396.c","EDB-ID":13396},

{"Exploit":"Linux/x86 - reboot() Shellcode (20 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13397.c","EDB-ID":13397},

{"Exploit":"Linux/x86 - setreuid(0\_ 0) + execve(/bin/sh) Shellcode (31 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13398.c","EDB-ID":13398},

{"Exploit":"Linux/x86 - execve(/bin/sh) / PUSH Shellcode (23 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13399.c","EDB-ID":13399},

{"Exploit":"Linux/x86 - cat /dev/urandom > /dev/console Shellcode (63 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13400.c","EDB-ID":13400},

{"Exploit":"Linux/x86 - Connect Back Shellcode (90 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13401.c","EDB-ID":13401},

{"Exploit":"Linux/x86 - socket-proxy Shellcode (372 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13402.c","EDB-ID":13402},

{"Exploit":"Linux/x86 - dup2(0\_0); dup2(0\_1); dup2(0\_2); Shellcode (15 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13403.c","EDB-ID":13403},

{"Exploit":"Linux/x86 - if(read(fd\_buf\_512)<=2) \_exit(1) else buf(); Shellcode (29 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13404.c","EDB-ID":13404},

{"Exploit":"Linux/x86 - \_exit(1); Shellcode (7 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13405.c","EDB-ID":13405},

{"Exploit":"Linux/x86 - read(0\_buf\_2541); chmod(buf\_4755); Shellcode (23 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13406.c","EDB-ID":13406},

{"Exploit":"Linux/x86 - write(0\_\_Hello core!\n\_\_12); (with optional 7 byte exit) Shellcode (36 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13407.c","EDB-ID":13407},

{"Exploit":"Linux/x86 - snoop /dev/dsp Shellcode (172 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13408.c","EDB-ID":13408},

{"Exploit":"Linux/x86 - /bin/sh Standard Opcode Array Payload Shellcode (21 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13409.c","EDB-ID":13409},

{"Exploit":"Linux/x86 - examples of long-term payloads hide-wait-change Shellcode (.s) (187+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13410.s","EDB-ID":13410},

{"Exploit":"Linux/x86 - examples of long-term payloads hide-wait-change Shellcode (187+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13411.c","EDB-ID":13411},

{"Exploit":"Linux/x86 - /bin/sh sysenter Opcode Array Payload Shellcode (23 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13412.c","EDB-ID":13412},

{"Exploit":"Linux/x86 - /bin/sh sysenter Opcode Array Payload Shellcode (27 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13413.c","EDB-ID":13413},

{"Exploit":"Linux/x86 - /bin/sh sysenter Opcode Array Payload Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13414.c","EDB-ID":13414},

{"Exploit":"Linux/x86 - chroot & standart Shellcode (66 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13415.c","EDB-ID":13415},

{"Exploit":"Linux/x86 - upload & exec Shellcode (189 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13416.txt","EDB-ID":13416},

{"Exploit":"Linux/x86 - setreuid/execve Shellcode (31 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13417.c","EDB-ID":13417},

{"Exploit":"Linux/x86 - alpha-numeric Shellcode (64 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13418.c","EDB-ID":13418},

{"Exploit":"Linux/x86 - alpha-numeric using IMUL Method Shellcode (88 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13419.c","EDB-ID":13419},

{"Exploit":"Linux/x86 - Radically Self Modifying Code Shellcode (70 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13420.c","EDB-ID":13420},

{"Exploit":"Linux/x86 - Magic Byte Self Modifying Code Shellcode (76 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13421.c","EDB-ID":13421},

{"Exploit":"Linux/x86 - execve code Shellcode (23 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13422.c","EDB-ID":13422},

{"Exploit":"Linux/x86 - execve(\_/bin/ash\_\_0\_0); Shellcode (21 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13423.c","EDB-ID":13423},

{"Exploit":"Linux/x86 - execve /bin/sh alphanumeric Shellcode (392 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13424.txt","EDB-ID":13424},

{"Exploit":"Linux/x86 - execve /bin/sh IA32 0xff-less Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13425.c","EDB-ID":13425},

{"Exploit":"Linux/x86 - symlink /bin/sh xoring Shellcode (56 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13426.c","EDB-ID":13426},

{"Exploit":"Linux/x86 - portbind port 5074 toupper Shellcode (226 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13427.c","EDB-ID":13427},

{"Exploit":"Linux/x86 - Add user 't00r' encrypt Shellcode (116 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13428.c","EDB-ID":13428},

{"Exploit":"Linux/x86 - chmod 666 shadow ENCRYPT Shellcode (75 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13429.c","EDB-ID":13429},

{"Exploit":"Linux/x86 - symlink . /bin/sh Shellcode (32 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13430.c","EDB-ID":13430},

{"Exploit":"Linux/x86 - kill snort Shellcode (151 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13431.c","EDB-ID":13431},

{"Exploit":"Linux/x86 - shared memory exec Shellcode (50 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13432.c","EDB-ID":13432},

{"Exploit":"Linux/x86 - iptables -F Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13433.c","EDB-ID":13433},

{"Exploit":"Linux/x86 - iptables -F Shellcode (58 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13434.c","EDB-ID":13434},

{"Exploit":"Linux/x86 - Reverse telnet Shellcode (134 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13435.c","EDB-ID":13435},

{"Exploit":"Linux/x86 - connect Shellcode (120 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13436.c","EDB-ID":13436},

{"Exploit":"Linux/x86 - chmod 666 /etc/shadow Shellcode (41 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13437.c","EDB-ID":13437},

{"Exploit":"Linux/x86 - cp /bin/sh /tmp/katy ; chmod 4555 katy Shellcode (126 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13438.c","EDB-ID":13438},

{"Exploit":"Linux/x86 - eject /dev/cdrom Shellcode (64 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13439.c","EDB-ID":13439},

{"Exploit":"Linux/x86 - xterm -ut -display [IP]:0 Shellcode (132 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13440.c","EDB-ID":13440},

{"Exploit":"Linux/x86 - ipchains -F Shellcode (49 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13441.c","EDB-ID":13441},

{"Exploit":"Linux/x86 - chmod 666 /etc/shadow Shellcode (82 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13442.c","EDB-ID":13442},

{"Exploit":"Linux/x86 - execve /bin/sh Shellcode (29 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13443.c","EDB-ID":13443},

{"Exploit":"Linux/x86 - execve /bin/sh Shellcode (24 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13444.c","EDB-ID":13444},

{"Exploit":"Linux/x86 - execve /bin/sh Shellcode (38 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13445.c","EDB-ID":13445},

{"Exploit":"Linux/x86 - execve /bin/sh Shellcode (30 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13446.c","EDB-ID":13446},

{"Exploit":"Linux/x86 - execve /bin/sh setreuid(12\_12) Shellcode (50 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13447.c","EDB-ID":13447},

{"Exploit":"Linux/x86 - portbind port 5074 Shellcode (92 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13448.c","EDB-ID":13448},

{"Exploit":"Linux/x86 - portbind port 5074 + fork() Shellcode (130 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13449.c","EDB-ID":13449},

{"Exploit":"Linux/x86 - Add user 't00r' Shellcode (82 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13450.c","EDB-ID":13450},

{"Exploit":"Linux/x86 - Add user Shellcode (104 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13451.c","EDB-ID":13451},

{"Exploit":"Linux/x86 - break chroot Shellcode (34 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13452.c","EDB-ID":13452},

{"Exploit":"Linux/x86 - break chroot Shellcode (46 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13453.c","EDB-ID":13453},

{"Exploit":"Linux/x86 - break chroot execve /bin/sh Shellcode (80 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13454.c","EDB-ID":13454},

{"Exploit":"Linux/x86 - execve /bin/sh encrypted Shellcode (58 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13455.c","EDB-ID":13455},

{"Exploit":"Linux/x86 - execve /bin/sh xor encrypted Shellcode (55 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13456.c","EDB-ID":13456},

{"Exploit":"Linux/x86 - execve /bin/sh tolower() evasion Shellcode (41 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13457.c","EDB-ID":13457},

{"Exploit":"Linux/x86 - execve of /bin/sh after setreuid(0\_0) Shellcode (46+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13458.c","EDB-ID":13458},

{"Exploit":"Linux/x86 - chroot()/execve() code Shellcode (80 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13459.c","EDB-ID":13459},

{"Exploit":"Linux/x86 - execve /bin/sh toupper() evasion Shellcode (55 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13460.c","EDB-ID":13460},

{"Exploit":"Linux/x86 - Add User 'z' Shellcode (70 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13461.c","EDB-ID":13461},

{"Exploit":"Linux/x86 - break chroot setuid(0) + /bin/sh Shellcode (132 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13462.c","EDB-ID":13462},

{"Exploit":"Linux/x86-64 - bindshell port 4444 Shellcode (132 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/13463.c","EDB-ID":13463},

{"Exploit":"Linux/x86-64 - execve(/bin/sh) Shellcode (33 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/13464.s","EDB-ID":13464},

{"Exploit":"Linux PPC & x86 - execve(\_/bin/sh\_\_{\_/bin/sh\_\_NULL}\_NULL) Shellcode (99 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/shellcode/13465.c","EDB-ID":13465},

{"Exploit":"Linux/x86 & Unix/SPARC & IRIX/MIPS - execve /bin/sh Shellcode (141 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/shellcode/13467.c","EDB-ID":13467},

{"Exploit":"Linux/x86 & Unix/SPARC - execve /bin/sh Shellcode (80 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/shellcode/13468.c","EDB-ID":13468},

{"Exploit":"Linux/x86 & bsd/x86 - execve /bin/sh Shellcode (38 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/shellcode/13469.c","EDB-ID":13469},

{"Exploit":"Linux/x86 - kill all processes Shellcode (9 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13548.asm","EDB-ID":13548},

{"Exploit":"Linux/x86 - setuid(0) & execve(\_/sbin/poweroff -f\_) Shellcode (47 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13549.c","EDB-ID":13549},

{"Exploit":"Linux/x86 - setuid(0) and cat /etc/shadow Shellcode (49 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13550.c","EDB-ID":13550},

{"Exploit":"Linux/x86 - chmod(/etc/shadow\_ 0666) & exit() Shellcode (33 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13551.c","EDB-ID":13551},

{"Exploit":"Linux/x86 - Linux/x86 execve() Shellcode (51 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13553.c","EDB-ID":13553},

{"Exploit":"Linux/x86 - overwrite MBR on /dev/sda with \_LOL!' Shellcode (43 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13563.asm","EDB-ID":13563},

{"Exploit":"Linux/x86 - setreuid (0\_0) & execve(/bin/rm /etc/shadow) Shellcode","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13566.c","EDB-ID":13566},

{"Exploit":"Linux/x86 - unlink(/etc/passwd) & exit() Shellcode (35 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13572.c","EDB-ID":13572},

{"Exploit":"Linux/x86 - chmod 666 /etc/shadow Shellcode (27 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13576.asm","EDB-ID":13576},

{"Exploit":"Linux/x86 - break chroot Shellcode (79 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13577.txt","EDB-ID":13577},

{"Exploit":"Linux/x86 - fork bomb Shellcode (6 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13578.txt","EDB-ID":13578},

{"Exploit":"Linux/x86 - append '/etc/passwd' & exit() Shellcode (107 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13579.c","EDB-ID":13579},

{"Exploit":"Linux/x86 - eject /dev/cdrom Shellcode (42 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13586.txt","EDB-ID":13586},

{"Exploit":"Linux/x86 - polymorphic Shellcode ip6tables -F (71 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13599.txt","EDB-ID":13599},

{"Exploit":"Linux/x86 - ip6tables -F Shellcode (47 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13600.txt","EDB-ID":13600},

{"Exploit":"Linux/i686 - pacman -S <package> (default package: backdoor) Shellcode (64 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13601.txt","EDB-ID":13601},

{"Exploit":"Linux/i686 - pacman -R <package> Shellcode (59 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13602.txt","EDB-ID":13602},

{"Exploit":"Linux/x86 - bin/cat /etc/passwd Shellcode (43 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13609.c","EDB-ID":13609},

{"Exploit":"Linux/x86 - /bin/sh Shellcode (8 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13627.c","EDB-ID":13627},

{"Exploit":"Linux/x86 - execve /bin/sh Shellcode (21 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13628.c","EDB-ID":13628},

{"Exploit":"Linux/x86 - disabled modsecurity Shellcode (64 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13632.c","EDB-ID":13632},

{"Exploit":"Linux/x86 - nc -lvve/bin/sh -p13377 Shellcode","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13661.txt","EDB-ID":13661},

{"Exploit":"Linux/x86 - chmod(\_/etc/shadow\_\_ 0666) Shellcode (36 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13669.c","EDB-ID":13669},

{"Exploit":"Linux/x86-64 - execve(\_/bin/sh\_) Shellcode (25 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/13670.c","EDB-ID":13670},

{"Exploit":"Linux/x86 - DoS-Badger-Game Shellcode (6 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13671.c","EDB-ID":13671},

{"Exploit":"Linux/x86 - SLoc-DoS Shellcode (55 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13673.c","EDB-ID":13673},

{"Exploit":"Linux/x86 - execve(\_a->/bin/sh\_) Local-only Shellcode (14 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13675.c","EDB-ID":13675},

{"Exploit":"Linux/x86 - chmod(\_/etc/shadow\_\_ 0777) Shellcode (33 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13676.c","EDB-ID":13676},

{"Exploit":"Linux/x86 - chmod(\_/etc/shadow\_\_ 0777) Shellcode (29 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13677.c","EDB-ID":13677},

{"Exploit":"Linux - write() & exit(0) Shellcode genearator with customizable text","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/13679.py","EDB-ID":13679},

{"Exploit":"Linux/x86 - polymorphic forkbombe Shellcode (30 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13680.c","EDB-ID":13680},

{"Exploit":"Linux/x86 - forkbomb Shellcode (6 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13681.c","EDB-ID":13681},

{"Exploit":"Linux/x86 - setreud(getuid()\_ getuid()) & execve(\_/bin/sh\_) Shellcode (34 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13682.c","EDB-ID":13682},

{"Exploit":"Linux/x86-64 - reboot(POWER\_OFF) Shellcode (19 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/13688.c","EDB-ID":13688},

{"Exploit":"Linux/x86-64 - execve(\_/bin/sh\_); Shellcode (30 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/13691.c","EDB-ID":13691},

{"Exploit":"Linux/x86 - sends 'Phuck3d!' to all terminals Shellcode (60 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13692.c","EDB-ID":13692},

{"Exploit":"Linux/x86 - execve(\_/bin/bash\_\_\_-p\_\_NULL) Shellcode (33 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13697.c","EDB-ID":13697},

{"Exploit":"Linux/x86 - polymorphic execve(\_/bin/bash\_\_\_-p\_\_NULL) Shellcode (57 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13698.c","EDB-ID":13698},

{"Exploit":"Linux/x86 - execve(\_/usr/bin/wget\_\_ \_aaaa\_); Shellcode (42 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13702.c","EDB-ID":13702},

{"Exploit":"Linux/x86 - sys\_execve(\_/bin/sh\_\_ \_0\_\_ \_0\_) with umask 16 (sys\_umask(14)) Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13703.txt","EDB-ID":13703},

{"Exploit":"Linux/x86 - Disable randomize stack addresse Shellcode (106 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13712.c","EDB-ID":13712},

{"Exploit":"Linux/x86 - pwrite(\_/etc/shadow\_\_ hash\_ 32\_ 8) Shellcode (83 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13715.c","EDB-ID":13715},

{"Exploit":"Linux/x86 - alphanumeric Bomb FORK Shellcode (117 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13716.c","EDB-ID":13716},

{"Exploit":"Linux/x86 - Polymorphic setuid(0) + chmod(\_/etc/shadow\_\_ 0666) Shellcode (61 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13722.c","EDB-ID":13722},

{"Exploit":"Linux/x86 - change mode 0777 of '/etc/shadow' with sys\_chmod syscall Shellcode (39 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13723.c","EDB-ID":13723},

{"Exploit":"Linux/x86 - kill all running process Shellcode (11 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13724.c","EDB-ID":13724},

{"Exploit":"Linux/x86 - change mode 0777 of '/etc/passwd' with sys\_chmod syscall Shellcode (39 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13725.txt","EDB-ID":13725},

{"Exploit":"Linux/x86 - sys\_execve(\_/bin/sh\_\_ \_-c\_\_ \_reboot\_) Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13726.txt","EDB-ID":13726},

{"Exploit":"Linux/x86 - sys\_setuid(0) & sys\_setgid(0) & execve (\_/bin/sh\_) Shellcode (39 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13728.c","EDB-ID":13728},

{"Exploit":"Linux/x86 - unlink \_/etc/shadow\_ Shellcode (33 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13730.c","EDB-ID":13730},

{"Exploit":"Linux/x86 - hard / unclean reboot Shellcode (29 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13731.c","EDB-ID":13731},

{"Exploit":"Linux/x86 - hard / unclean reboot Shellcode (33 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13732.c","EDB-ID":13732},

{"Exploit":"Linux/x86 - chown root:root /bin/sh Shellcode (48 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13742.c","EDB-ID":13742},

{"Exploit":"Linux/x86 - give all user root access when execute /bin/sh Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13743.c","EDB-ID":13743},

{"Exploit":"Linux/x86 - netcat connect back port 8080 Shellcode (76 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/14334.c","EDB-ID":14334},

{"Exploit":"Linux/x86-64 - Disable ASLR Security Shellcode (143 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/13908.c","EDB-ID":13908},

{"Exploit":"Linux/x86 - Polymorphic Bindport 31337 with setreuid (0\_0) Shellcode (131 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/13910.c","EDB-ID":13910},

{"Exploit":"Linux/x86-64 - setuid(0) & chmod (\_/etc/passwd\_\_ 0777) & exit(0) Shellcode (63 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/13915.txt","EDB-ID":13915},

{"Exploit":"Linux/x86-64 - Add root user \_shell-storm\_ with password \_leet\_ Shellcode (390 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/13943.c","EDB-ID":13943},

{"Exploit":"Linux/ARM - setuid(0) & kill(-1\_ SIGKILL) Shellcode (28 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/14116.txt","EDB-ID":14116},

{"Exploit":"Linux/ARM - execve(\_/bin/sh\_\_\_/bin/sh\_\_0) Shellcode (30 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/14097.c","EDB-ID":14097},

{"Exploit":"Linux/x86 - Polymorphic /bin/sh Shellcode (116 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/14119.c","EDB-ID":14119},

{"Exploit":"Linux/ARM - polymorphic chmod(\_/etc/shadow\_\_ 0777) Shellcode (84 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/14142.c","EDB-ID":14142},

{"Exploit":"Linux/ARM - chmod(\_/etc/shadow\_\_ 0777) Shellcode (35 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/14122.txt","EDB-ID":14122},

{"Exploit":"Linux/ARM - Disable ASLR Security Shellcode (102 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/14139.c","EDB-ID":14139},

{"Exploit":"Linux/ARM - Polymorphic execve(\_/bin/sh\_\_ [\_/bin/sh\_]\_ NULL); - XOR 88 encoded Shellcode (78 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/14190.c","EDB-ID":14190},

{"Exploit":"Linux/x86 - bind shell port 64533 Shellcode (97 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/14216.c","EDB-ID":14216},

{"Exploit":"Linux - Drop suid shell root in /tmp/.hiddenshell Polymorphic Shellcode (161 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/14218.c","EDB-ID":14218},

{"Exploit":"Linux - setreuid(0\_0) execve(\_/bin/sh\_\_NULL\_NULL) XOR Encoded Shellcode (62 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/14219.c","EDB-ID":14219},

{"Exploit":"Linux - 125 bind port to 6778 XOR encoded polymorphic Shellcode (125 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/14234.c","EDB-ID":14234},

{"Exploit":"Linux - \_nc -lp 31337 -e /bin//sh\_ polymorphic Shellcode (91 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/14235.c","EDB-ID":14235},

{"Exploit":"Linux - Find all writeable folder in filesystem polymorphic Shellcode (91 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/14276.c","EDB-ID":14276},

{"Exploit":"Linux/x86-64 - execve(\_/sbin/iptables\_\_ [\_/sbin/iptables\_\_ \_-F\_]\_ NULL) Shellcode (49 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/14305.c","EDB-ID":14305},

{"Exploit":"Linux/x86 - netcat bindshell port 8080 Shellcode (75 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/14332.c","EDB-ID":14332},

{"Exploit":"Linux/x86 - /bin/sh Polymorphic Null Free Shellcode (46 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/14691.c","EDB-ID":14691},

{"Exploit":"Linux/ARM - execve(\_/bin/sh\_\_ [0]\_ [0 vars]) Shellcode (27 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/14907.c","EDB-ID":14907},

{"Exploit":"Linux/ARM - Add root user 'shell-storm' with password 'toor' Shellcode (151 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/15616.c","EDB-ID":15616},

{"Exploit":"Linux/SuperH (sh4) - setuid(0) / chmod(\_/etc/shadow\_\_ 0666) / exit(0) Shellcode (43 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sh4/shellcode/17432.c","EDB-ID":17432},

{"Exploit":"Linux/x86 - netcat bindshell port 6666 Shellcode (69 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/17194.txt","EDB-ID":17194},

{"Exploit":"Linux/x86 - ASLR deactivation Shellcode (83 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/20195.c","EDB-ID":20195},

{"Exploit":"Linux/x86 - ConnectBack with SSL connection Shellcode (422 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/17371.txt","EDB-ID":17371},

{"Exploit":"Linux/SuperH (sh4) - Add root user 'shell-storm' with password 'toor' Shellcode (143 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sh4/shellcode/17439.c","EDB-ID":17439},

{"Exploit":"Linux/x86 - egghunt Shellcode (29 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/17559.c","EDB-ID":17559},

{"Exploit":"Linux/MIPS - execve Shellcode (52 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/17940.c","EDB-ID":17940},

{"Exploit":"Linux/MIPS - XOR Shellcode Encoder (60 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/17996.c","EDB-ID":17996},

{"Exploit":"Linux/SuperH (sh4) - setuid(0) ; execve(\_/bin/sh\_\_ NULL\_ NULL) Shellcode (27 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/sh4/shellcode/18154.c","EDB-ID":18154},

{"Exploit":"Linux/MIPS - execve /bin/sh Shellcode (48 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/18162.c","EDB-ID":18162},

{"Exploit":"Linux/MIPS - Add user(UID 0) 'rOOt' with password 'pwn3d' Shellcode (164 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/18163.c","EDB-ID":18163},

{"Exploit":"Linux/x86-64 - execve(/bin/sh) Shellcode (52 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/18197.c","EDB-ID":18197},

{"Exploit":"Linux/MIPS - connect back Shellcode (port 0x7a69) (168 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/18226.c","EDB-ID":18226},

{"Exploit":"Linux/MIPS - reboot() Shellcode (32 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/18227.c","EDB-ID":18227},

{"Exploit":"Linux/x86 - Polymorphic Shellcode setuid(0) + setgid(0) + add user \_iph\_ without password to /etc/passwd","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/18294.c","EDB-ID":18294},

{"Exploit":"Linux/x86 - Search For php/html Writable Files and Add Your Code Shellcode (380+ bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/18379.c","EDB-ID":18379},

{"Exploit":"Linux/x86-64 - Add user \_t0r\_ with password \_Winner\_ Shellcode (189 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/18585.s","EDB-ID":18585},

{"Exploit":"Linux/x86 - execve(/bin/dash) Shellcode (42 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/18885.c","EDB-ID":18885},

{"Exploit":"Linux/x86 - chmod 666 /etc/passwd & /etc/shadow Shellcode (57 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/20196.c","EDB-ID":20196},

{"Exploit":"Linux/ARM (Raspberry Pi) - reverse\_shell (tcp\_10.1.1.2\_0x1337) Shellcode (72 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/21252.asm","EDB-ID":21252},

{"Exploit":"Linux/ARM (Raspberry Pi) - execve(\_/bin/sh\_\_ [0]\_ [0 vars]) Shellcode (30 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/21253.asm","EDB-ID":21253},

{"Exploit":"Linux/ARM (Raspberry Pi) - chmod(\_/etc/shadow\_\_ 0777) Shellcode (41 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/21254.asm","EDB-ID":21254},

{"Exploit":"Linux/x86 - Remote Port Forwarding Shellcode (87 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/23622.c","EDB-ID":23622},

{"Exploit":"Linux/x86 - Reverse TCP Bind 192.168.1.10:31337 Shellcode (92 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/25497.c","EDB-ID":25497},

{"Exploit":"Linux/x86 - Egg-hunter Shellcode (31 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40827.c","EDB-ID":40827},

{"Exploit":"Linux/x86 - Multi-Egghunter Shellcode","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/28474.c","EDB-ID":28474},

{"Exploit":"Linux/MIPS (Little Endian) - Reverse Shell (192.168.1.177:31337) Shellcode (200 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/29436.asm","EDB-ID":29436},

{"Exploit":"Linux/x86 - Socket Re-use Shellcode (50 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/34060.c","EDB-ID":34060},

{"Exploit":"Linux/x86 - chmod (777 /etc/passwd & /etc/shadow)\_ Add New Root User (ALI/ALI) & Execute /bin/sh Shellcode (378 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/34262.c","EDB-ID":34262},

{"Exploit":"Linux/x86 - Obfuscated Shellcode chmod 777 (/etc/passwd + /etc/shadow) & Add New Root User \_ALI\_ & Execute /bin/bash (521 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/34592.c","EDB-ID":34592},

{"Exploit":"Linux/x86-64 - Connect Back Shellcode (139 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/34667.c","EDB-ID":34667},

{"Exploit":"Linux/x86 - Add map in /etc/hosts file (google.com 127.1.1.1) Shellcode (77 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/34778.c","EDB-ID":34778},

{"Exploit":"Linux/x86-64 - Position independent & Alphanumeric execve(\_/bin/sh\0\_\_NULL\_NULL); Shellcode (87 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/35205.txt","EDB-ID":35205},

{"Exploit":"Linux/x86 - rmdir Shellcode (37 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/35519.txt","EDB-ID":35519},

{"Exploit":"Linux/x86-64 - Bind 4444/TCP Port Shellcode (81 bytes / 96 bytes with password)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/35586.c","EDB-ID":35586},

{"Exploit":"Linux/x86-64 - Reverse TCP connect Shellcode (77 to 85 bytes / 90 to 98 bytes with password)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/35587.c","EDB-ID":35587},

{"Exploit":"Linux/MIPS - execve /bin/sh Shellcode (36 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/35868.c","EDB-ID":35868},

{"Exploit":"Linux/MIPS (Little Endian) - Chmod 666 /etc/shadow Shellcode (55 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/36274.c","EDB-ID":36274},

{"Exploit":"Linux/MIPS (Little Endian) - Chmod 666 /etc/passwd Shellcode (55 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_mips/shellcode/36276.c","EDB-ID":36276},

{"Exploit":"Linux/x86-64 - Reads Data From /etc/passwd To /tmp/outfile Shellcode (118 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/36359.c","EDB-ID":36359},

{"Exploit":"Linux/x86 - ROT13 encoded execve(\_/bin/sh\_) Shellcode (68 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36391.c","EDB-ID":36391},

{"Exploit":"Linux/x86 - chmod 0777 /etc/shadow obfuscated Shellcode (84 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36393.c","EDB-ID":36393},

{"Exploit":"Linux/x86 - Obfuscated map google.com to 127.1.1.1 Shellcode (98 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36394.c","EDB-ID":36394},

{"Exploit":"Linux/x86 - Obfuscated execve(\_/bin/sh\_) Shellcode (40 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36395.c","EDB-ID":36395},

{"Exploit":"Linux/x86 - Reverse TCP Shell Shellcode (72 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36397.c","EDB-ID":36397},

{"Exploit":"Linux/x86 - Bind Shell 33333/TCP Port Shellcode (96 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36398.c","EDB-ID":36398},

{"Exploit":"Linux/x86 - Disable ASLR Shellcode (84 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36637.c","EDB-ID":36637},

{"Exploit":"Linux/x86 - Egg-hunter Shellcode (20 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36672.asm","EDB-ID":36672},

{"Exploit":"Linux/x86 - Typewriter Shellcode (Generator)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36673.py","EDB-ID":36673},

{"Exploit":"Linux/x86 - Create 'my.txt' Working Directory Shellcode (37 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36701.c","EDB-ID":36701},

{"Exploit":"Linux/x86 - setreuid(0\_ 0) + execve(\_/sbin/halt\_) + exit(0) Shellcode (49 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36750.c","EDB-ID":36750},

{"Exploit":"Linux/x86 - execve \_/bin/sh\_ Shellcode (35 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36778.c","EDB-ID":36778},

{"Exploit":"Linux/x86 - custom execve-Shellcode Encoder/Decoder","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36781.py","EDB-ID":36781},

{"Exploit":"Linux/x86 - Execve /bin/sh Shellcode Via Push (21 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36857.c","EDB-ID":36857},

{"Exploit":"Linux/x86-64 - Execve /bin/sh Shellcode Via Push (23 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/36858.c","EDB-ID":36858},

{"Exploit":"Linux/x86 - /bin/nc -le /bin/sh -vp 17771 Shellcode (58 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36921.c","EDB-ID":36921},

{"Exploit":"Linux/x86 - exit(0) Shellcode (6 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/36908.c","EDB-ID":36908},

{"Exploit":"Linux/x86 - execve \_/bin/sh\_ Shellcode (26 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37069.c","EDB-ID":37069},

{"Exploit":"Linux/x86 - execve /bin/sh Shellcode (21 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37251.asm","EDB-ID":37251},

{"Exploit":"Linux/x86 - chmod() 777 /etc/shadow & exit() Shellcode (33 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37285.txt","EDB-ID":37285},

{"Exploit":"Linux/x86 - execve /bin/sh Shellcode (2) (21 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37289.txt","EDB-ID":37289},

{"Exploit":"Linux/x86 - /etc/passwd Reader Shellcode (58 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37297.txt","EDB-ID":37297},

{"Exploit":"Linux/x86 - mkdir HACK & chmod 777 and exit(0) Shellcode (29 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37358.c","EDB-ID":37358},

{"Exploit":"Linux/x86 - Netcat BindShell Port 5555 Shellcode (60 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37359.c","EDB-ID":37359},

{"Exploit":"Linux/x86-64 - execve(/bin/sh) Shellcode (30 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/37362.c","EDB-ID":37362},

{"Exploit":"Linux/x86 - Download & Execute Shellcode","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37365.c","EDB-ID":37365},

{"Exploit":"Linux/x86 - Reboot Shellcode (28 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37366.c","EDB-ID":37366},

{"Exploit":"Linux/x86 - execve /bin/sh Shellcode (23 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37384.c","EDB-ID":37384},

{"Exploit":"Linux/x86 - chmod('/etc/passwd'\_0777) Shellcode (42 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37390.asm","EDB-ID":37390},

{"Exploit":"Linux/x86 - chmod('/etc/gshadow') Shellcode (37 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37391.asm","EDB-ID":37391},

{"Exploit":"Linux/x86 - chmod('/etc/shadow'\_'0777') Shellcode (42 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37392.asm","EDB-ID":37392},

{"Exploit":"Linux/x86 - exec('/bin/dash') Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37393.asm","EDB-ID":37393},

{"Exploit":"Linux/x86-64 - Encoded execve Shellcode (57 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/37401.asm","EDB-ID":37401},

{"Exploit":"Linux/x86-64 - encoded execve Shellcode (57 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/37427.txt","EDB-ID":37427},

{"Exploit":"Linux/x86 - /bin/sh ROT7 Encoded Shellcode","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37495.py","EDB-ID":37495},

{"Exploit":"Linux/x86 - Egg Hunter Shellcode (19 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37749.c","EDB-ID":37749},

{"Exploit":"Linux/x86 - /bin/sh ROL/ROR Encoded Shellcode","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/37762.py","EDB-ID":37762},

{"Exploit":"Linux/x86 - execve(/bin/bash) Shellcode (31 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/38088.c","EDB-ID":38088},

{"Exploit":"Linux/x86 - Create file with permission 7775 and exit Shellcode (Generator)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/38094.c","EDB-ID":38094},

{"Exploit":"Linux/x86 - execve(\_/bin/cat\_\_ [\_/bin/cat\_\_ \_/etc/passwd\_]\_ NULL) Shellcode (75 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/38116.c","EDB-ID":38116},

{"Exploit":"Linux/x86-64 - /bin/sh Shellcode (34 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/38150.txt","EDB-ID":38150},

{"Exploit":"Linux/x86-64 - execve Shellcode (22 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/38239.asm","EDB-ID":38239},

{"Exploit":"Linux/x86-64 - Bindshell 31173 port with Password Shellcode (92 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/38469.c","EDB-ID":38469},

{"Exploit":"Linux/x86-64 - egghunter Shellcode (24 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/38708.asm","EDB-ID":38708},

{"Exploit":"Linux/x86-64 - Polymorphic execve Shellcode (31 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/38815.c","EDB-ID":38815},

{"Exploit":"Linux/x86-64 - Bind TCP Port Shellcode (103 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39149.c","EDB-ID":39149},

{"Exploit":"Linux/x86-64 - Bind 4444/TCP Port Shellcode (103 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39151.c","EDB-ID":39151},

{"Exploit":"Linux/x86-64 - Bindshell 4444/TCP with Password Prompt Shellcode (162 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39152.c","EDB-ID":39152},

{"Exploit":"Linux/x86 - execve \_/bin/sh\_ Shellcode (24 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/39160.c","EDB-ID":39160},

{"Exploit":"Linux/x86-64 - TCP Reverse Shell with Password Prompt Shellcode (151 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39185.c","EDB-ID":39185},

{"Exploit":"Linux/x86-64 - Egghunter Shellcode (18 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39203.c","EDB-ID":39203},

{"Exploit":"Linux/x86 - Egg-hunter Shellcode (13 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/39204.c","EDB-ID":39204},

{"Exploit":"Linux/x86-64 - xor/not/div Encoded execve Shellcode (54 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39312.c","EDB-ID":39312},

{"Exploit":"Linux x86 / x86\_64 - reverse\_tcp (192.168.1.29:4444) Shellcode (195 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/39336.c","EDB-ID":39336},

{"Exploit":"Linux x86 / x86\_64 - tcp\_bind (Port 4444) Shellcode (251 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/39337.c","EDB-ID":39337},

{"Exploit":"Linux x86 / x86\_64 - Read /etc/passwd Shellcode (156 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/39338.c","EDB-ID":39338},

{"Exploit":"Linux/x86-64 - shell\_reverse\_tcp with Password Polymorphic Shellcode (1) (122 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39383.c","EDB-ID":39383},

{"Exploit":"Linux/x86-64 - shell\_reverse\_tcp with Password Polymorphic Shellcode (2) (135 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39388.c","EDB-ID":39388},

{"Exploit":"Linux/x86 - Download & Execute Shellcode (135 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/39389.c","EDB-ID":39389},

{"Exploit":"Linux/x86-64 - Polymorphic Execve-Stack Shellcode (47 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39390.c","EDB-ID":39390},

{"Exploit":"Linux/ARM - Connect back to 10.0.0.10:1337 with /bin/sh Shellcode (95 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/arm/shellcode/39496.c","EDB-ID":39496},

{"Exploit":"Linux/x86-64 - Reverse Shell Shellcode (134 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39578.c","EDB-ID":39578},

{"Exploit":"Linux/x86-64 - execve(/bin/sh) Shellcode (26 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39617.c","EDB-ID":39617},

{"Exploit":"Linux/x86-64 - execve(/bin/sh) Shellcode (25 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39624.c","EDB-ID":39624},

{"Exploit":"Linux/x86-64 - execve(/bin/bash) Shellcode (33 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39625.c","EDB-ID":39625},

{"Exploit":"Linux/x86-64 - bindshell (Port 5600) Shellcode (81 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39684.c","EDB-ID":39684},

{"Exploit":"Linux/x86-64 - Read /etc/passwd Shellcode (65 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39700.c","EDB-ID":39700},

{"Exploit":"Linux/x86-64 - bindshell (Port 5600) Shellcode (86 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39718.c","EDB-ID":39718},

{"Exploit":"Linux/x86 - Reverse TCP Shellcode (IPv6) (159 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/39722.c","EDB-ID":39722},

{"Exploit":"Linux/x86 - Bind TCP Port 1472 (IPv6) Shellcode (1250 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/39723.c","EDB-ID":39723},

{"Exploit":"Linux/x86-64 - Bind Shell Shellcode (Generator)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39728.py","EDB-ID":39728},

{"Exploit":"Linux/x86-64 - Bind 1472/TCP Shellcode (IPv6) (199 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39758.c","EDB-ID":39758},

{"Exploit":"Linux/x86-64 - Reverse TCP Shellcode (IPv6) (203 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39763.c","EDB-ID":39763},

{"Exploit":"Linux/x86 - Bindshell with Configurable Port Shellcode (87 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/39815.c","EDB-ID":39815},

{"Exploit":"Linux/x86-64 - Reverse TCP Shell Null Free Shellcode (134 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39844.c","EDB-ID":39844},

{"Exploit":"Linux/x86-64 - Information Stealer Shellcode (399 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39847.c","EDB-ID":39847},

{"Exploit":"Linux/x86 - Bind Shell Port 4444/TCP Shellcode (656 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/39851.c","EDB-ID":39851},

{"Exploit":"Linux/x86-64 - XOR Encode execve Shellcode (84 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/39869.c","EDB-ID":39869},

{"Exploit":"Linux/Windows/BSD x86\_64 - execve(\_/bin//sh\_\_ {\_//bin/sh\_\_ \_-c\_\_ \_cmd\_}\_ NULL) Execute Command Shellcode (194 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/shellcode/39885.c","EDB-ID":39885},

{"Exploit":"Linux/x86 - /bin/nc -le /bin/sh -vp13337 Shellcode (56 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/39901.c","EDB-ID":39901},

{"Exploit":"Linux/x86 - /bin/sh Shellcode + ASLR Bruteforce","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40026.txt","EDB-ID":40026},

{"Exploit":"Linux/x86-64 - /etc/passwd File Sender Shellcode (164 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/40029.c","EDB-ID":40029},

{"Exploit":"Linux/x86-64 - NetCat Bind Shell Shellcode (64 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/40052.c","EDB-ID":40052},

{"Exploit":"Linux/x86 - Bind Shell Port 4444/TCP Shellcode (98 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40056.c","EDB-ID":40056},

{"Exploit":"Linux/x86-64 - Ncat Shellcode (SSL\_ MultiChannel\_ Persistant\_ Fork\_ IPv4/6\_ Password) (176 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/40061.c","EDB-ID":40061},

{"Exploit":"Linux/x86 - TCP Reverse Shellcode (75 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40075.c","EDB-ID":40075},

{"Exploit":"Linux/x86-64 - Continuously-Probing Reverse Shell via Socket + Port-range + Password Shellcode (172 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/40079.c","EDB-ID":40079},

{"Exploit":"Linux/x86 - Reverse Shell using Xterm ///usr/bin/xterm -display 127.1.1.1:10 Shellcode (68 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40110.c","EDB-ID":40110},

{"Exploit":"Linux/x86-64 - Syscall Persistent Bind Shell / Multi-terminal / Password / Daemon Shellcode (83\_ 148\_ 177 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/40122.txt","EDB-ID":40122},

{"Exploit":"Linux/CRISv32 - Axis Communication Connect Back Shellcode (189 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux\_crisv32/shellcode/40128.c","EDB-ID":40128},

{"Exploit":"Linux/x86 - execve /bin/sh Shellcode (19 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40131.c","EDB-ID":40131},

{"Exploit":"Linux/x86-64 - Subtle Probing Reverse Shell / Timer\_ Burst / Password / Multi-Terminal Shellcode (84\_ 122\_ 172 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/40139.c","EDB-ID":40139},

{"Exploit":"Linux/x86 - NetCat Bind Shellcode with Port (44 / 52 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40179.c","EDB-ID":40179},

{"Exploit":"Linux/x86 - zsh TCP Port 9090 Bind Shellcode (96 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40222.c","EDB-ID":40222},

{"Exploit":"Linux/x86 - zsh Reverse TCP Shellcode port 9090 (80 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40223.c","EDB-ID":40223},

{"Exploit":"Linux/x86-64 - /bin/sh -c reboot Shellcode (89 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/40808.c","EDB-ID":40808},

{"Exploit":"Linux/x86 - Netcat (-e option disabled) Reverse Shell Shellcode (180 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40872.c","EDB-ID":40872},

{"Exploit":"Linux/x86 - /bin/bash -c Arbitrary Command Execution Shellcode (72 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/40924.c","EDB-ID":40924},

{"Exploit":"Linux/x86-64 - mkdir Shellcode (25 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/41089.c","EDB-ID":41089},

{"Exploit":"Linux/x86-64 - Bind 5600 TCP Port - Shellcode (87 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/41128.c","EDB-ID":41128},

{"Exploit":"Linux/x86-64 - execve /bin/sh Shellcode (22 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/41174.nasm","EDB-ID":41174},

{"Exploit":"Linux - Multi/Dual mode execve(\_/bin/sh\_\_ NULL\_ 0) Shellcode (37 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/41183.c","EDB-ID":41183},

{"Exploit":"Linux - Multi/Dual mode Reverse Shell Shellcode (129 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/41220.c","EDB-ID":41220},

{"Exploit":"Linux/x86 - Reverse TCP Alphanumeric Staged Shellcode (103 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/41282.nasm","EDB-ID":41282},

{"Exploit":"Linux - Dual/Multi mode Bind Shell Shellcode (156 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/41375.c","EDB-ID":41375},

{"Exploit":"Linux - TCP Reverse Shell Shellcode (65 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/41398.nasm","EDB-ID":41398},

{"Exploit":"Linux/x86 - SELinux Permissive Mode Switcher Shellcode (45 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/41403.c","EDB-ID":41403},

{"Exploit":"Linux/x86-64 - Egghunter Shellcode (38 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/41439.c","EDB-ID":41439},

{"Exploit":"Linux/x86-64 - Random Listener Shellcode (54 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/41468.nasm","EDB-ID":41468},

{"Exploit":"Linux/x86-64 - Reverse Shell Shellcode (84 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/shellcode/41477.c","EDB-ID":41477},

{"Exploit":"Linux/x86-64 - Polymorphic Setuid(0) & Execve(/bin/sh) Shellcode (31 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/41498.nasm","EDB-ID":41498},

{"Exploit":"Linux/x86-64 - Polymorphic Flush IPTables Shellcode (47 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/41503.nasm","EDB-ID":41503},

{"Exploit":"Linux/x86-64 - NetCat Reverse Shell Shellcode (72 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/41509.nasm","EDB-ID":41509},

{"Exploit":"Linux/x86-64 - Polymorphic NetCat Reverse Shell Shellcode (106 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/41510.nsam","EDB-ID":41510},

{"Exploit":"Linux/x86 - Encoded exceve(\_/bin/sh\_) Shellcode (44 Bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/41630.asm","EDB-ID":41630},

{"Exploit":"Linux/x86 - Bind Shell Shellcode (44 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/41631.c","EDB-ID":41631},

{"Exploit":"Linux/x86 - File Reader Shellcode (54 Bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/41635.txt","EDB-ID":41635},

{"Exploit":"Linux/x86 - Reverse /bin/bash Shellcode (110 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/41723.c","EDB-ID":41723},

{"Exploit":"Linux/x86-64 - execve(\_/bin/sh\_) Shellcode (21 Bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/shellcode/41750.txt","EDB-ID":41750},

{"Exploit":"Linux/x86 - execve(/bin/sh\_) Shellcode (19 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/41757.txt","EDB-ID":41757},

{"Exploit":"Invision Gallery 2.0.7 (Linux) - readfile() / SQL Injection","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/php/webapps/2527.c","EDB-ID":2527},

{"Exploit":"webSPELL 4.2.0d (Linux) - Local File Disclosure (C)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/php/webapps/8559.c","EDB-ID":8559},

{"Exploit":"Enigma2 Webinterface 1.7.x 1.6.x 1.5.x - (linux) Remote File Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/webapps/18343.pl","EDB-ID":18343},

{"Exploit":"LinuxStat 2.x - Directory Traversal","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/cgi/webapps/24703.txt","EDB-ID":24703},

{"Exploit":"ClarkConnect Linux 5.0 - 'proxy.php' Cross-Site Scripting","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/php/webapps/33435.txt","EDB-ID":33435}

]

}

searchsploit -tj linux remote

{

"SEARCH": "linux remote",

"RESULTS": [

{"Exploit":"Apache 2.0.44 (Linux) - Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/11.c","EDB-ID":11},

{"Exploit":"Linux Kernel < 2.6.16.18 - Netfilter NAT SNMP Module Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/1880.c","EDB-ID":1880},

{"Exploit":"Linux Kernel 2.6.21.1 - IPv6 Jumbo Bug Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/4893.c","EDB-ID":4893},

{"Exploit":"Psi Jabber Client (Windows / Linux) - (8010/tcp) Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/dos/7555.py","EDB-ID":7555},

{"Exploit":"Linux Kernel < 2.6.30.5 - 'cfg80211' Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/9442.c","EDB-ID":9442},

{"Exploit":"Linux Kernel 2.6.33.3 - SCTP INIT Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/14594.py","EDB-ID":14594},

{"Exploit":"Linux 2.6.36 IGMP - Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/18378.c","EDB-ID":18378},

{"Exploit":"Linux Kernel 2.6.x - IPTables Logging Rules Integer Underflow Remote (PoC)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/24696.c","EDB-ID":24696},

{"Exploit":"Linux Kernel 2.6.17.7 - NFS and EXT3 Combination Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/28358.txt","EDB-ID":28358},

{"Exploit":"Linux-HA Heartbeat 2.0.6 - Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/28386.txt","EDB-ID":28386},

{"Exploit":"Linux Kernel 2.6.22 - IPv6 Hop-By-Hop Header Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/30902.c","EDB-ID":30902},

{"Exploit":"Linux Kernel 2.6.35 - Network Namespace Remote Denial of Service","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/36425.txt","EDB-ID":36425},

{"Exploit":"Linux eXtremail 1.5.x - Remote Format Strings Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/49.c","EDB-ID":49},

{"Exploit":"Real Server 7/8/9 (Windows / Linux) - Remote Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/86.c","EDB-ID":86},

{"Exploit":"Linux pam\_lib\_smb < 1.1.6 - /bin/login Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/89.c","EDB-ID":89},

{"Exploit":"BeroFTPD 1.3.4(1) (Linux x86) - Remote Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/remote/269.c","EDB-ID":269},

{"Exploit":"CVS (Linux/FreeBSD) - Remote Entry Line Heap Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/300.c","EDB-ID":300},

{"Exploit":"Linux imapd - Remote Overflow File Retrieve Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/340.c","EDB-ID":340},

{"Exploit":"SHOUTcast DNAS/Linux 1.9.4 - Format String Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/712.c","EDB-ID":712},

{"Exploit":"Medal of Honor Spearhead (Linux) - Server Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/826.c","EDB-ID":826},

{"Exploit":"Ethereal 0.10.9 (Linux) - '3G-A11' Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/878.c","EDB-ID":878},

{"Exploit":"RealPlayer/Helix Player (Linux) - Remote Format String","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/1232.c","EDB-ID":1232},

{"Exploit":"Veritas NetBackup 6.0 (Linux) - (bpjava-msvc) Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/1263.pl","EDB-ID":1263},

{"Exploit":"linux-ftpd-ssl 0.17 - 'MKD'/'CWD' Remote Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/1295.c","EDB-ID":1295},

{"Exploit":"Snort 2.6.1 (Linux) - DCE/RPC Preprocessor Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/3609.py","EDB-ID":3609},

{"Exploit":"3proxy 0.5.3g (Linux) - proxy.c logurl() Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/3821.c","EDB-ID":3821},

{"Exploit":"Debian OpenSSH - Authenticated Remote SELinux Privilege Elevation Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/6094.txt","EDB-ID":6094},

{"Exploit":"Linux Kernel 2.6.20 / 2.6.24 / 2.6.27\_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora Core 10 / OpenSuse 11.1) - SCTP FWD Memory Corruption Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/8556.c","EDB-ID":8556},

{"Exploit":"McAfee LinuxShield 1.5.1 - Local/Remote File Inclusion (Remote Code Execution)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/14818.pl","EDB-ID":14818},

{"Exploit":"HP Data Protector (Linux) - Remote Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/17648.sh","EDB-ID":17648},

{"Exploit":"Linuxconf 1.1.6 r10 - Remote Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20619.c","EDB-ID":20619},

{"Exploit":"RedHat Linux 7.0 Apache - Remote 'Username' Enumeration","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/21112.php","EDB-ID":21112},

{"Exploit":"HP SiteScope (Linux/Windows) - Remote Code Execution (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/21137.rb","EDB-ID":21137},

{"Exploit":"Antologic Antolinux 1.0 - Administrative Interface NDCR Parameter Remote Command Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/23604.txt","EDB-ID":23604},

{"Exploit":"Nginx 1.4.0 (x64) (Generic Linux) - Remote Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86-64/remote/32277.txt","EDB-ID":32277},

{"Exploit":"Linux/MIPS Kernel 2.6.36 - 'NetUSB' Remote Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/38454.py","EDB-ID":38454},

{"Exploit":"Xdh / LinuxNet Perlbot / fBot IRC Bot - Remote Code Execution (Metasploit)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/multiple/remote/38974.rb","EDB-ID":38974},

{"Exploit":"McAfee Virus Scan Enterprise for Linux 1.9.2 < 2.0.2 - Remote Code Execution","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/40911.py","EDB-ID":40911},

{"Exploit":"Linux/x86 - Remote Port Forwarding Shellcode (87 bytes)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/lin\_x86/shellcode/23622.c","EDB-ID":23622},

{"Exploit":"Enigma2 Webinterface 1.7.x 1.6.x 1.5.x - (linux) Remote File Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/webapps/18343.pl","EDB-ID":18343}

]

}

searchsploit -tj debian 5

{

"SEARCH": "debian 5",

"RESULTS": [

{"Exploit":"Linux Kernel 2.0.x (Debian 2.1 / RedHat 5.2) - Packet Length with Options","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/dos/19675.c","EDB-ID":19675},

{"Exploit":"BSD/OS 2.1 / DG/UX 7.0 / Debian 1.3 / HP-UX 10.34 / IBM AIX 4.2 / SGI IRIX 6.4 / Solaris 2.5.1 - xlock Exploit (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19172.c","EDB-ID":19172},

{"Exploit":"BSD/OS 2.1 / DG/UX 7.0 / Debian 1.3 / HP-UX 10.34 / IBM AIX 4.2 / SGI IRIX 6.4 / Solaris 2.5.1 - xlock Exploit (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19173.c","EDB-ID":19173},

{"Exploit":"BSD/OS 2.1 / DG/UX 4.0 / Debian 0.93 / Digital UNIX 4.0 B / FreeBSD 2.1.5 / HP-UX 10.34 / IBM AIX 4.1.5 / NetBSD 1.0/1.1 / NeXTstep 4.0 / SGI IRIX 6.3 / SunOS 4.1.4 - rlogin Exploit","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/19203.c","EDB-ID":19203},

{"Exploit":"Debian 2.0/2.0 r5 / FreeBSD 3.2 / OpenBSD 2.4 / RedHat 5.2 i386 / S.u.S.E. 6.1 - Lsof Buffer Overflow (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19373.c","EDB-ID":19373},

{"Exploit":"Debian 2.0/2.0 r5 / FreeBSD 3.2 / OpenBSD 2.4 / RedHat 5.2 i386 / S.u.S.E. 6.1 - Lsof Buffer Overflow (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19374.c","EDB-ID":19374},

{"Exploit":"gpm 1.18.1/1.19 / Debian 2.x / RedHat 6.x / S.u.S.E 5.3/6.x - gpm Setgid","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/19816.txt","EDB-ID":19816},

{"Exploit":"Debian 2.x / RedHat 6.2 / IRIX 5/6 / Solaris 2.x - Mail Reply-To Field","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/local/20382.pl","EDB-ID":20382},

{"Exploit":"Linux Kernel 2.6.32-5 (Debian 6.0.5) - /dev/ptmx Key Stroke Timing Local Disclosure","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/local/24459.sh","EDB-ID":24459},

{"Exploit":"Conectiva 4.x/5.x / Debian 2.x / RedHat 6.x / S.u.S.E 6.x/7.0 / Trustix 1.x - rpc.statd Remote Format String (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20075.c","EDB-ID":20075},

{"Exploit":"Conectiva 4.x/5.x / Debian 2.x / RedHat 6.x / S.u.S.E 6.x/7.0 / Trustix 1.x - rpc.statd Remote Format String (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20076.c","EDB-ID":20076},

{"Exploit":"Conectiva 4.x/5.x / Debian 2.x / RedHat 6.x / S.u.S.E 6.x/7.0 / Trustix 1.x - rpc.statd Remote Format String (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20077.c","EDB-ID":20077},

{"Exploit":"Solaris 2.x/7.0/8 / IRIX 6.5.x / OpenBSD 2.x / NetBSD 1.x / Debian 3 / HP-UX 10 - TelnetD Buffer Overflow","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/unix/remote/21018.c","EDB-ID":21018}

]

}

searchsploit -tj debian 5 remote

{

"SEARCH": "debian 5 remote",

"RESULTS": [

{"Exploit":"Conectiva 4.x/5.x / Debian 2.x / RedHat 6.x / S.u.S.E 6.x/7.0 / Trustix 1.x - rpc.statd Remote Format String (1)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20075.c","EDB-ID":20075},

{"Exploit":"Conectiva 4.x/5.x / Debian 2.x / RedHat 6.x / S.u.S.E 6.x/7.0 / Trustix 1.x - rpc.statd Remote Format String (2)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20076.c","EDB-ID":20076},

{"Exploit":"Conectiva 4.x/5.x / Debian 2.x / RedHat 6.x / S.u.S.E 6.x/7.0 / Trustix 1.x - rpc.statd Remote Format String (3)","Path":"/usr/local/Cellar/exploitdb/2016-12-24/share/exploitdb/platforms/linux/remote/20077.c","EDB-ID":20077}

]

}