Fedora 21 apache 2.4, php 5, and mariaDB/mysql server installed:

[\*] FINDING RELEVENT PRIVILEGE ESCALATION EXPLOITS…

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a ‘\*\*’ but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mounted file system

* MySQL 4.x/5.0 User Defined Function Local Privilege Escalation Exploit :: <http:///www.exploit-db.com/exploits/1518> :: Language=c

The following exploits are applicable to this kernel version and should be investigated as well:

* Kernel ia32syscall Emulation Privilege Escalation :: <http://www.exploit-db.com/exploits/15023> :: Language=c
* Sendpage Local Privilege Escalation :: <http://www.exploit-db.com/exploits/19933> :: Language=ruby\*\*
* CAP\_SYS\_ADMIN to Root Exploit 2 (32 and 64-bit) :: <http://www.exploit-db.com/exploits/15944> :: Language=c
* CAP\_SYS\_ADMIN to root Exploit :: <http://www.exploit-db.com/exploits/15916> :: Language=c
* MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit :: <http://www.exploit-db.com/exploits/1518> Language=c
* open-time Capability file\_ns\_capable() Privilege Escalation :: <http://www.exploit-db.com/exploits/25450> :: Language=c
* open-time Capability file\_ns\_capable() – Privilege Escalation Vulnerability :: <http://www.exploit-db.com/exploits/25307> :: Language=c

Ubuntu 12.04 with bind9:

[\*] FINDING RELEVENT PRIVILEGE ESCALATION EXPLOITS…

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a ‘\*\*’ but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mounted file system

The following exploits are applicable to this kernel version and should be investigated as well:

* Kernel ia32syscall Emulation Privilege Escalation :: <http://www.exploit-db.com/exploits/15023> :: Language=c
* Sendpage Local Privilege Escalation :: <http://www.exploit-db.com/exploits/19933> :: Language=ruby\*\*
* CAP\_SYS\_ADMIN to Root Exploit 2 (32 and 64-bit) :: <http://www.exploit-db.com/exploits/15944> :: Language=c
* CAP\_SYS\_ADMIN to root Exploit :: <http://www.exploit-db.com/exploits/15916> :: Language=c
* MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit :: <http://www.exploit-db.com/exploits/1518> Language=c
* open-time Capability file\_ns\_capable() Privilege Escalation :: <http://www.exploit-db.com/exploits/25450> :: Language=c
* open-time Capability file\_ns\_capable() – Privilege Escalation Vulnerability :: <http://www.exploit-db.com/exploits/25307> :: Language=c

CentOS 6.4 splunk box:

[\*] FINDING RELEVENT PRIVILEGE ESCALATION EXPLOITS…

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a ‘\*\*’ but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mounted file system

* 2.6 UDEV < 141 Local Privilege Escalation Exploit :: <http://www.exploit-db.com/exploits/8572> :: Language=c
* 2.6 UDEV Local Privilege Escalation Exploit :: <http://www.exploit-db.com/exploits8478> :: Language=c

The following exploits are applicable to this kernel version and should be investigated as well

* Kernel ia32syscall Emulation Privilege Escalation :: <http://www.exploit-db.com/exploits/15023> :: Language=c
* Sendpage Local Privilege Escalation :: <http://www.exploit-db.com/exploits/19933> :: Language=ruby\*\*
* 2.x sock\_sendpage() Local Root Exploit 2 :: <http://www.exploit-db.com/exploits/9436> :: Language=c
* 2.4/2.6 sock\_sendpage() ring0 Root Exploit (simple ver) :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9479 :: Language=c
* 2.x sock\_sendpage() Local Ring0 Root Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9435 :: Language=c
* CAP\_SYS\_ADMIN to Root Exploit 2 (32 and 64-bit) :: <http://www.exploit-db.com/exploits/15944> :: Language=c
* Linux RDS Protocol Local Privilege Escalation :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)15285 :: Language=c
* 2.6.x ptrace\_attach Local Privlege Escalation Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)8673 :: Language=c
* 2.4/2.6 bluez Local Root Privilege Escalation Exploit (update) :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)926 :: Language=c
* CAP\_SYS\_ADMIN to root Exploit :: <http://www.exploit-db.com/exploits/15916> :: Language=c
* 2.6 UDEV Local Privilege Escalation Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)8478 :: Language=c
* MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit :: <http://www.exploit-db.com/exploits/1518> Language=c
* < 2.6.36.2 Econet Privilege Escalation Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)17787 :: Language=c
* ‘pipe.c’ Local Privilege Escalation Vulnerability :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)10018 :: Language=sh
* <= 2.6.37 Local Privilege Escalation :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)15704 :: Language=c
* open-time Capability file\_ns\_capable() Privilege Escalation :: <http://www.exploit-db.com/exploits/25450> :: Language=c
* 2.4.1-2.4.37 and 2.6.1-2.6.32-rc5 Pipe.c Privilege Escalation :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9844 :: Language=python
* open-time Capability file\_ns\_capable() – Privilege Escalation Vulnerability :: <http://www.exploit-db.com/exploits/25307> :: Language=c
* 2.4/2.6 sock\_sendpage() Local Root Exploit [2] :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9598 :: Language=c
* < 2.6.36-rc1 CAN BCM Privilege Escalation Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)14814 :: Language=c
* 2.4/2.6 sock\_sendpage() Local Root Exploit (ppc) :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9545 :: Language=c
* < 2.6.37-rc2 ACPI custom\_method Privilege Escalation :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)15774 :: Language=c
* 2.4/2.6 sock\_sendpage() Local Root Exploit[3] :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9641 :: Language=c
* 2.4.x / 2.6.x uselib() Local Privilege Escalation Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)895 :: Language=c

CentOS 7 for phantom. Base install:

[\*] FINDING RELEVENT PRIVILEGE ESCALATION EXPLOITS…

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a ‘\*\*’ but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mounted file system

The following exploits are applicable to this kernel version and should be investigated as well:

* Kernel ia32syscall Emulation Privilege Escalation :: <http://www.exploit-db.com/exploits/15023> :: Language=c
* Sendpage Local Privilege Escalation :: <http://www.exploit-db.com/exploits/19933> :: Language=ruby\*\*
* CAP\_SYS\_ADMIN to Root Exploit 2 (32 and 64-bit) :: <http://www.exploit-db.com/exploits/15944> :: Language=c
* CAP\_SYS\_ADMIN to root Exploit :: <http://www.exploit-db.com/exploits/15916> :: Language=c
* MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit :: <http://www.exploit-db.com/exploits/1518> Language=c
* open-time Capability file\_ns\_capable() Privilege Escalation :: <http://www.exploit-db.com/exploits/25450> :: Language=c
* open-time Capability file\_ns\_capable() – Privilege Escalation Vulnerability :: <http://www.exploit-db.com/exploits/25307> :: Language=c

CentOS 6 with httpd, mysql, and php installed:

[\*] FINDING RELEVENT PRIVILEGE ESCALATION EXPLOITS…

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a ‘\*\*’ but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mounted file system

* 2.6 UDEV < 141 Local Privilege Escalation Exploit :: <http://www.exploit-db.com/exploits/8572> :: Language=c
* 2.6 UDEV Local Privilege Escalation Exploit :: <http://www.exploit-db.com/exploits8478> :: Language=c

The following exploits are applicable to this kernel version and should be investigated as well

* Kernel ia32syscall Emulation Privilege Escalation :: <http://www.exploit-db.com/exploits/15023> :: Language=c
* Sendpage Local Privilege Escalation :: <http://www.exploit-db.com/exploits/19933> :: Language=ruby\*\*
* 2.x sock\_sendpage() Local Root Exploit 2 :: <http://www.exploit-db.com/exploits/9436> :: Language=c
* 2.4/2.6 sock\_sendpage() ring0 Root Exploit (simple ver) :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9479 :: Language=c
* 2.x sock\_sendpage() Local Ring0 Root Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9435 :: Language=c
* CAP\_SYS\_ADMIN to Root Exploit 2 (32 and 64-bit) :: <http://www.exploit-db.com/exploits/15944> :: Language=c
* Linux RDS Protocol Local Privilege Escalation :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)15285 :: Language=c
* 2.6.x ptrace\_attach Local Privlege Escalation Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)8673 :: Language=c
* 2.4/2.6 bluez Local Root Privilege Escalation Exploit (update) :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)926 :: Language=c
* CAP\_SYS\_ADMIN to root Exploit :: <http://www.exploit-db.com/exploits/15916> :: Language=c
* 2.6 UDEV Local Privilege Escalation Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)8478 :: Language=c
* MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit :: <http://www.exploit-db.com/exploits/1518> Language=c
* < 2.6.36.2 Econet Privilege Escalation Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)17787 :: Language=c
* ‘pipe.c’ Local Privilege Escalation Vulnerability :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)10018 :: Language=sh
* <= 2.6.37 Local Privilege Escalation :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)15704 :: Language=c
* open-time Capability file\_ns\_capable() Privilege Escalation :: <http://www.exploit-db.com/exploits/25450> :: Language=c
* 2.4.1-2.4.37 and 2.6.1-2.6.32-rc5 Pipe.c Privilege Escalation :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9844 :: Language=python
* open-time Capability file\_ns\_capable() – Privilege Escalation Vulnerability :: <http://www.exploit-db.com/exploits/25307> :: Language=c
* 2.4/2.6 sock\_sendpage() Local Root Exploit [2] :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9598 :: Language=c
* < 2.6.36-rc1 CAN BCM Privilege Escalation Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)14814 :: Language=c
* 2.4/2.6 sock\_sendpage() Local Root Exploit (ppc) :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9545 :: Language=c
* < 2.6.37-rc2 ACPI custom\_method Privilege Escalation :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)15774 :: Language=c
* 2.4/2.6 sock\_sendpage() Local Root Exploit[3] :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)9641 :: Language=c
* 2.4.x / 2.6.x uselib() Local Privilege Escalation Exploit :: [http://www.exploit-db.com/exploits/](http://www.exploit-db.com/exploits/946)895 :: Language=c

Debian 7.8 mysql installed:

[\*] FINDING RELEVENT PRIVILEGE ESCALATION EXPLOITS…

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a ‘\*\*’ but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mounted file system

* Debian OpenSSL Predictable PRNG Bruteforce SSH Exploit :: <http://www.exploit-db.com/exploits/5720> :: Language=python

The following exploits are applicable to this kernel version and should be investigated as well:

* Kernel ia32syscall Emulation Privilege Escalation :: <http://www.exploit-db.com/exploits/15023> :: Language=c
* Sendpage Local Privilege Escalation :: <http://www.exploit-db.com/exploits/19933> :: Language=ruby\*\*
* CAP\_SYS\_ADMIN to Root Exploit 2 (32 and 64-bit) :: <http://www.exploit-db.com/exploits/15944> :: Language=c
* CAP\_SYS\_ADMIN to root Exploit :: <http://www.exploit-db.com/exploits/15916> :: Language=c
* MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit :: <http://www.exploit-db.com/exploits/1518> Language=c
* open-time Capability file\_ns\_capable() Privilege Escalation :: <http://www.exploit-db.com/exploits/25450> :: Language=c
* open-time Capability file\_ns\_capable() – Privilege Escalation Vulnerability :: <http://www.exploit-db.com/exploits/25307> :: Language=c