Linux Commands Cheat Sheet ∞

CHEAT-SHEET 02 Nov 2014  Arr0way

A collection of hopefully useful Linux Commands for pen testers, this is not a complete list but a collection of commonly used commands + syntax as a sort of "cheatsheet", this content will be constantly updated as I discover new awesomeness.

Table of Contents

Linux Penetration Testing Commands

Linux Network Commands

COMMAND	DESCRIPTION
`netstat -tulpn`	Show Linux network ports with process ID's

	(PIDs)
`watch ss -stplu`	Watch TCP, UDP open ports in real time with socket summary.
`lsof -i`	Show established connections.
`macchanger -m MACADDR INTR`	Change MAC address on KALI Linux.
`ifconfig eth0 192.168.2.1/24`	Set IP address in Linux.
`ifconfig eth0:1 192.168.2.3/24`	Add IP address to existing network interface in Linux.
`ifconfig eth0 hw ether MACADDR`	Change MAC address in Linux using ifconfig.
`ifconfig eth0 mtu 1500`	Change MTU size Linux using ifconfig, change 1500 to your desired MTU.
`dig -x 192.168.1.1`	Dig reverse lookup on an IP address.
`host 192.168.1.1`	Reverse lookup on an IP address, in case dig is not installed.
`dig @192.168.2.2 domain.com -t AXFR`	Perform a DNS zone transfer using dig.
`host -l domain.com nameserver`	Perform a DNS zone transfer using host.
`nbtstat -A x.x.x.x`	Get hostname for IP address.
	Adds a hidden IP address to Linux, does

Writeup
InsomniHack CTF Teaser - Smartcat1 Writeup
FristiLeaks 1.3 Walkthrough
SickOS 1.1 - Walkthrough
The Wall Boot2Root Walkthrough
More »

TECHNIQUES

SSH & Meterpreter Pivoting Techniques
More »

SECURITY HARDENING

Security Harden CentOS 7
More »

/DEV/URANDOM

MacBook - Post Install Config + Apps
More »

OTHER BLOG

HowTo: Kali

`ip addr add 192.168.2.22/24 dev eth0`	not show up when performing an ifconfig.
`tcpkill -9 host google.com`	Blocks access to google.com from the host machine.
`echo "1" > /proc/sys/net/ipv4/ip_forward`	Enables IP forwarding, turns Linux box into a router - handy for routing traffic through a box.
`echo "8.8.8.8" > /etc/resolv.conf`	Use Google DNS.

System Information Commands

Useful for local enumeration.

COMMAND	DESCRIPTION
`whoami`	Shows currently logged in user on Linux.
`id`	Shows currently logged in user and groups for the user.
`last`	Shows last logged in users.
`mount`	Show mounted drives.
`df -h`	Shows disk usage in human readable output.
`echo "user:passwd" | chpasswd`	Reset password in one line.
`getent passwd`	List users on Linux.
`strings /usr/local/bin/blah`	Shows contents of none text files, e.g. whats in a binary.
`uname -ar`	Shows running kernel version.

`PATH=$PATH:/my/new-path`	Add a new PATH, handy for local FS manipulation.
`history`	Show bash history, commands the user has entered previously.

Redhat / CentOS / RPM Based Distros

COMMAND	DESCRIPTION
`cat /etc/redhat-release`	Shows Redhat / CentOS version number.
`rpm -qa`	List all installed RPM's on an RPM based Linux distro.
`rpm -q --changelog openvpn`	Check installed RPM is patched against CVE, grep the output for CVE.

YUM Commands

Package manager used by RPM based systems, you can pull some usefull information about installed packages and or install additional tools.

COMMAND	DESCRIPTION
`yum update`	Update all RPM packages with YUM, also shows whats out of date.
`yum update httpd`	Update individual packages, in this example HTTPD (Apache).
`yum install package`	Install a package using YUM.
`yum --exclude=package kernel* update`	Exclude a package from being updates with YUM.
`yum remove package`	Remove package with YUM.
`yum erase package`	Remove package with YUM.
	Lists info about yum

`yum list package`	package.
`yum provides httpd`	What a packages does, e.g Apache HTTPD Server.
`yum info httpd`	Shows package info, architecture, version etc.
`yum localinstall blah.rpm`	Use YUM to install local RPM, settles deps from repo.
`yum deplist package`	Shows deps for a package.
`yum list installed | more`	List all installed packages.
`yum grouplist | more`	Show all YUM groups.
`yum groupinstall 'Development Tools'`	Install YUM group.

Debian / Ubuntu / .deb Based Distros

COMMAND	DESCRIPTION
`cat /etc/debian_version`	Shows Debian version number.
`cat /etc/*-release`	Shows Ubuntu version number.
`dpkg -l`	List all installed packages on Debian / .deb based Linux distro.

Linux User Management

COMMAND	DESCRIPTION
`useradd new-user`	Creates a new Linux user.
`passwd username`	Reset Linux user password, enter just `passwd` if you are root.
`deluser username`	Remove a Linux user.

Linux Decompression Commands

How to extract various archives (tar, zip, gzip, bzip2 etc) on Linux and some other tricks for searching inside of archives etc.

COMMAND	DESCRIPTION
`unzip archive.zip`	Extracts zip file on Linux.
`zipgrep *.txt archive.zip`	Search inside a .zip archive.
`tar xf archive.tar`	Extract tar file Linux.
`tar xvzf archive.tar.gz`	Extract a tar.gz file Linux.
`tar xjf archive.tar.bz2`	Extract a tar.bz2 file Linux.
`tar ztvf file.tar.gz | grep blah`	Search inside a tar.gz file.
`gzip -d archive.gz`	Extract a gzip file Linux.
`zcat archive.gz`	Read a gz file Linux without decompressing.
`zless archive.gz`	Same function as the `less` command for .gz archives.
`zgrep 'blah' /var/log/maillog*.gz`	Search inside .gz archives on Linux, search inside of compressed log files.
`vim file.txt.gz`	Use vim to read .txt.gz files (my personal favorite).
`upx -9 -o output.exe input.exe`	UPX compress .exe file Linux.

Linux Compression Commands

COMMAND	DESCRIPTION
`zip -r file.zip /dir/*`	Creates a .zip file on Linux.
`tar cf archive.tar files`	Creates a tar file on Linux.

`tar czf archive.tar.gz files`	Creates a tar.gz file on Linux.
`tar cjf archive.tar.bz2 files`	Creates a tar.bz2 file on Linux.
`gzip file`	Creates a file.gz file on Linux.

Linux File Commands

COMMAND	DESCRIPTION
`df -h blah`	Display size of file / dir Linux.
`diff file1 file2`	Compare / Show differences between two files on Linux.
`md5sum file`	Generate MD5SUM Linux.
`md5sum -c blah.iso.md5`	Check file against MD5SUM on Linux, assuming both file and .md5 are in the same dir.
`file blah`	Find out the type of file on Linux, also displays if file is 32 or 64 bit.
`dos2unix`	Convert Windows line endings to Unix / Linux.
`base64 < input-file > output-file`	Base64 encodes input file and outputs a Base64 encoded file called output-file.
`base64 -d < input-file > output-file`	Base64 decodes input file and outputs a Base64 decoded file called output-file.
`touch -r ref-file new-file`	Creates a new file using the timestamp data from the reference file, drop the -r to

	simply create a file.
`rm -rf`	Remove files and directories without prompting for confirmation.

Samba Commands

Connect to a Samba share from Linux.

```
$ smbmount //server/share /mnt/win -o user=username,passwo
$ smbclient -U user \\\\server\\share
$ mount -t cifs -o username=user,password=password //x.x.x
```

Breaking Out of Limited Shells

Credit to G0tmi1k for these (or wherever he stole them from!).

The Python trick:

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
echo os.system('/bin/bash')
```

```
/bin/sh -i
```

Misc Commands

COMMAND	DESCRIPTION
`init 6`	Reboot Linux from the command line.
`gcc -o output.c input.c`	Compile C code.
`gcc -m32 -o output.c input.c`	Cross compile C code, compile 32 bit binary on 64 bit Linux.
`unset HISTORYFILE`	Disable bash history logging.
`rdesktop X.X.X.X`	Connect to RDP server from Linux.

`kill -9 $$`	Kill current session.
`chown user:group blah`	Change owner of file or dir.
`chown -R user:group blah`	Change owner of file or dir and all underlying files / dirs - recersive chown.
`chmod 600 file`	Change file / dir permissions, see [Linux File System Permissons](#linux-file-system-permissions) for details.

Clear bash history:

```
$ ssh user@X.X.X.X | cat /dev/null > ~/.bash_history
```

Linux File System Permissions

VALUE	MEANING
`777`	`rwxrwxrwx` No restriction, global WRX any user can do anything.
`755`	`rwxr-xr-x` Owner has full access, others can read and execute the file.
`700`	`rwx------` Owner has full access, no one else has access.
`666`	`rw-rw-rw-` All users can read and write but not execute.
`644`	`rw-r--r--` Owner can read and write, everyone else can read.
`600`	`rw-------` Owner can read and write, everyone else has no access.

Linux File System

DIRECTORY	DESCRIPTION
`/`	/ also know as "slash" or the root.

`/bin`	Common programs, shared by the system, the system administrator and the users.
`/boot`	Boot files, boot loader (grub), kernels, vmlinuz
`/dev`	Contains references to system devices, files with special properties.
`/etc`	Important system config files.
`/home`	Home directories for system users.
`/lib`	Library files, includes files for all kinds of programs needed by the system and the users.
`/lost+found`	Files that were saved during failures are here.
`/mnt`	Standard mount point for external file systems.
`/media`	Mount point for external file systems (on some distros).
`/net`	Standard mount point for entire remote file systems - nfs.
`/opt`	Typically contains extra and third party software.
`/proc`	A virtual file system containing information about system resources.
`/root`	root users home dir.
`/sbin`	Programs for use by the system and the system administrator.
`/tmp`	Temporary space for use by the system, cleaned upon reboot.
`/usr`	Programs, libraries, documentation etc. for all user-related programs.
`/var`	Storage for all variable files and temporary files created by users, such as log files, mail queue, print spooler. Web servers, Databases etc.

Linux Interesting Files / Dir's

Places that are worth a look if you are attempting to privilege escalate / perform post exploitation.

DIRECTORY	DESCRIPTION
`/etc/passwd`	Contains local Linux users.
`/etc/shadow`	Contains local account password hashes.
`/etc/group`	Contains local account groups.
`/etc/init.d/`	Contains service init script - worth a look to see whats installed.
`/etc/hostname`	System hostname.
`/etc/network/interfaces`	Network interfaces.
`/etc/resolv.conf`	System DNS servers.
`/etc/profile`	System environment variables.
`~/.ssh/`	SSH keys.
`~/.bash_history`	Users bash history log.
`/var/log/`	Linux system log files are typically stored here.
`/var/adm/`	UNIX system log files are typically stored here.
`/var/log/apache2/access.log` `/var/log/httpd/access.log`	Apache access log file typical path.
`/etc/fstab`	File system mounts.

Twitter Facebook Google+ Reddit

Follow Arr0way

Twitter GitHub

Also...

You might want to read these

CATEGORY	POST NAME
cheat-sheet	Penetration Testing Tools Cheat Sheet
cheat-sheet	LFI Cheat Sheet
kali linux	HowTo: Kali Linux Chromium Install for Web App Pen Testing
walkthroughs	InsomniHack CTF Teaser - Smartcat2 Writeup
walkthroughs	InsomniHack CTF Teaser - Smartcat1 Writeup
walkthroughs	FristiLeaks 1.3 Walkthrough
walkthroughs	SickOS 1.1 - Walkthrough
walkthroughs	The Wall Boot2Root Walkthrough
walkthroughs	/dev/random: Sleepy Walkthrough CTF
walkthroughs	/dev/random Pipe walkthrough