MENU

SECURISM

All about Information Security

OSCP NOTES – PRIVILEGE ESCALATION (LINUX)

LYNIS

https://cisofy.com/lynis/

LINUX EXPLOIT SUGGESTOR

https://github.com/PenturaLabs/Linux_Exploit_Suggester

SHELL ESCAPE SEQUENCES

> *nmap–>–interactive*
>
> *vi–> :!bash*
>
> *vi–> :set shell=/bin/bash:shell*
>
> *awk–> awk 'BEGIN {system("/bin/bash")}'*
>
> *find–> find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' \;*
>
> *perl–> perl -e 'exec "/bin/bash";'*

COMMANDS USEFUL FOR GAINING INFORMATION :

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

BASICS OF PRIVILEGE ESCALATION METHODS :

http://www.doomedraven.com/2013/04/hacking-linux-part-i-privilege.html
http://www.rebootuser.com/?p=1623#.V0W5Pbp95JP

LINUX PRIV CHECKER

https://www.securitysift.com/download/linuxprivchecker.py

Here's an overview of this Linux privilege escalation script identified:

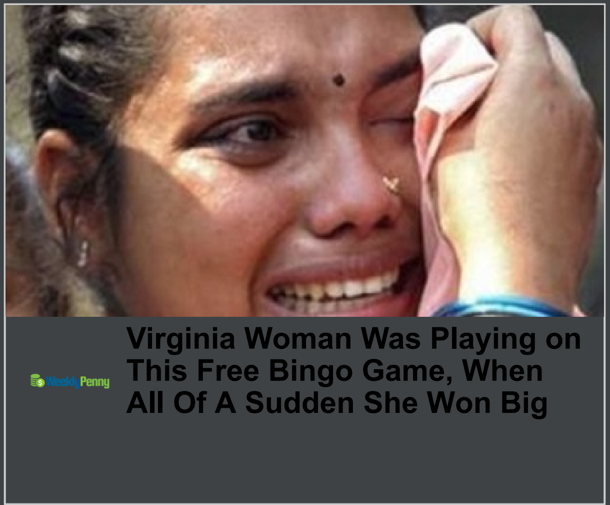
Basic system info (OS/Kernel/System name, etc)
Networking Info (ifconfig, route, netstat, etc)
Miscellaneous filesystem info (mount, fstab, cron jobs, etc)
User info (current user, all users, super users, command history, etc)
File and Directory permissions (world-writeable files/dirs, suid files, root home directory)
Files containing plaintext passwords
Interesting files, processes and applications (all processes and packages, all processes run by root and the associated packages, sudo version, apache config file, etc)
All installed languages and tools (gcc, perl, python, nmap, netcat, wget, ftp, etc)
All relevant privilege escalation exploits (using a comprehensive dictionary of exploits with applicable kernel versions, software packages/processes, etc)

UNIX PRIV ESC

> *./unix-priv-esc detailed > unix_priv_esc*

LINUX LOCAL EXPLOIT – UDEV

http://www.madirish.net/370
https://www.exploit-db.com/exploits/8572/



SHARE THIS:

Twitter Facebook

★ Like

Be the first to like this.

Search ...

PAGES

- Contact

- OSCP Notes – Buffer Overflow
- OSCP Notes – Exploitation
- OSCP Notes – File Transfers
- OSCP Notes – Information Gathering
- OSCP Notes – Meterpreter
- OSCP Notes – Password Attacks
- OSCP Notes – Port Forwarding
- OSCP Notes – Port Scanning
- OSCP Notes – Privilege Escalation (Linux)
- OSCP Notes – Privilege Escalation (Windows)
- OSCP Notes – Shells