( Cyber Spike CTF)

Joker CTF

Sudo sudoers shell privilege escalation

Inloggen op SSH server , kijken wat de inrichting/bestanden op het systeem zijn.

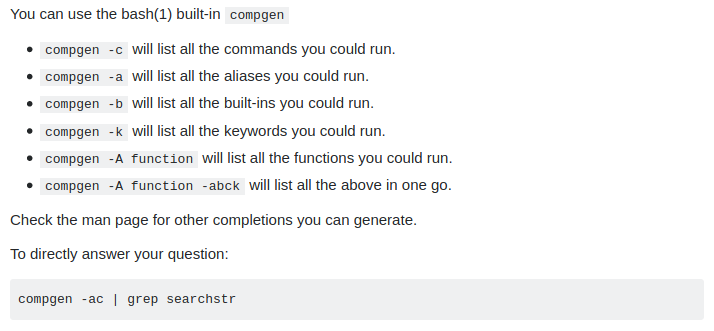
Service –status-all → Kijken welke services er draaien.

Controleren of ‘sudo’ werkt. Het resultaat is wijst uit dat de user (student) een sudoer is maar de toegestane commando’s zijn gelimiteerd.

student@server:~$ id rfadmin uid=1000(rfadmin) gid=1000(rfadmin) groups=1000(rfadmin),27(sudo) student@server:~$ id uid=1001(student) gid=1001(student) groups=1001(student),27(sudo)

Er is geen toegang tot de rootfolder. (niet met cat, ls, etc)

Hierna is ‘compgen -c ‘ gebruikt om te kijken welke commando’s gebruikt kunnen worden.



Patu-guide-linux-privilege-escalation.com → mogelijkheden voor privilige escalations. Echter hebben deze geen nut.

Als volgt is sudo -l gebruikt om te kijken welke commando’s die als root uitgevoerd kunnen worden.

(25 minuten zijn verstreken). Uit de output van sudo -l blijkt dat vim gebruikt kan worden om /etc/ motd aan te passen.

Met deze kennis wordt er onderzoek gedaan naar CVE’s die relevant zijn tot motd.

In de homefolder van student staat een verborgen bestand genaamd /sudo\_as\_admin\_succesful. Dit bestand wekt interesse. Het bestand is leeg. Enkele commando’s worden in het bestand gezet om te testen wat het resultaat is. Het is een doodlopend eind.

Ondertussen blijkt dat vi een afkorting/alternatieve naam voor vim is.

Met de gegeven informatie (motd aanpassen met vim) is er een poging om de sourcefile van vim aan te passen. Dit heeft geen resultaat.

De gevonden CVE van motd wijst uit dat symlink gedisabled moet zijn om eventuele ‘privilege escalations’ te kunnen doen. Hierbij komen we uit op het ‘linken’ in linux. Met name Symbolic links (symlink).

udev symlink → een service die links gebruikt.

[**systemd-udevd.service**](http://manpages.ubuntu.com/manpages/xenial/man8/systemd-udevd.service.8.html)

Om deze service uit te zetten wordt **systemctl disable udev.service gebruikt.**

De links tussen **vim en *etc*/alternatives/vim proberen we te verwijderen.** Dit kan niet.

Nog een poging is het aanmaken van een eigen script, om deze te kunnen linken aan e*tc*/alternatives/vim. Dit heeft geen resultaat.

Sudo vim *etc*motd is een van de mogelijkheden die getest is. Verschillende bestanden/commandos worden geprobeert om met vim uit te voeren.

Hieruit volgt dat de mogelijkheden binnen VIM ontdekt worden. Uiteindelijk blijkt dat bash commando’s uitgevoerd kunnen worden met de prefix van “:!”:

oplossing:

*Met vim kan motd aangepast worden, hier staat de flag.*

**Oplossing ‘:! cat *root*/flag.txt’**

Aanpassen ~/.bashrc file → geen resultaat

Linux kernel checking. Version 4.15.-88-generic

root is not allowed to execute → nieuwe user aanmaken heeft geen nut.

Commands:

crontab

chroot

id

geprobeerd:

sudo -l : commandos bruikbaar voor sudo user

Bruikbaar als sudo

motd

motd cv

motd privilege escalation if kernel symlink disabled:

udev symlink

[**systemd-udevd.service**](http://manpages.ubuntu.com/manpages/xenial/man8/systemd-udevd.service.8.html) **to stop: → systemctl disable udev.service**

oplossing:

*etc/motd is enigste uitvoerbaar als root.*

*Met vim kan motd aangepast worden, hier staat de flag.*

*commando’s gebruikt in vm*

*:!*

*the challenge*

*https://hub.rangeforce.com/lab/soc-challenge---joker*

[*https://fireshellsecurity.team/restricted-linux-shell-escaping-techniques/*](https://fireshellsecurity.team/restricted-linux-shell-escaping-techniques/)

compgen command

[*https://stackoverflow.com/questions/948008/linux-command-to-list-all-available-commands-and-aliases*](https://stackoverflow.com/questions/948008/linux-command-to-list-all-available-commands-and-aliases)

*btrfs system root guide*

[*https://wiki.gentoo.org/wiki/Btrfs/System\_Root\_Guide*](https://wiki.gentoo.org/wiki/Btrfs/System_Root_Guide)

*cheatsheet – write up*

[*https://pequalsnp-team.github.io/cheatsheet/writing-good-writeup*](https://pequalsnp-team.github.io/cheatsheet/writing-good-writeup)

*sudoers file*

[*https://www.linux.com/tutorials/configuring-linux-sudoers-file/*](https://www.linux.com/tutorials/configuring-linux-sudoers-file/)

*disallow shell escapes as a default*

[*https://unix.stackexchange.com/questions/473950/sudo-disallow-shell-escapes-as-a-default*](https://unix.stackexchange.com/questions/473950/sudo-disallow-shell-escapes-as-a-default)

*motd info:*

[*https://www.putorius.net/custom-motd-login-screen-linux.html*](https://www.putorius.net/custom-motd-login-screen-linux.html)

*edit motd:*

*https://access.redhat.com/solutions/223483*

*remove symbolic link*

*https://askubuntu.com/questions/398818/how-to-remove-symbolic-link*