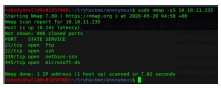
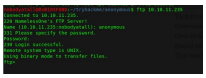
imgPOC

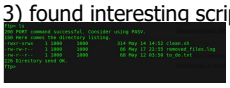
1) Scan open ports



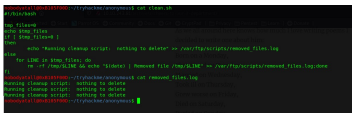
2) ftp able to login anonymously



3) found interesting script and log

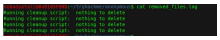


4) Seems like it's a script that will be execute to clean the tmp directory and after clean it will append the text either "Running cleanup script: nothing to delete" or "Removed file /tmp/...."" into /var/ftp/scripts/removed_files.log which is the removed_files.log in the ftp scripts directory

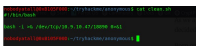


5) after some time it seems like the clean.sh triggered automatically, so i assume that there's a cron jobs running behind there.

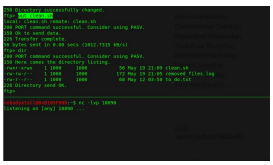
//previous img show's only 3 line in the log but after some time it become 4 line, so it means that the script has been executed and message append into the log



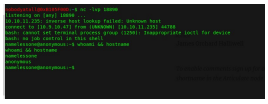
6) edit the clean.sh script with the reverse shell payload



7) upload the edited script into ftp server and wait for the reverse shell payload script to be executed

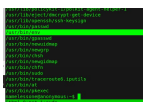


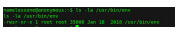
8) after the clean.sh executed, we got our reverse shell



9) check for suid binaries

10) found interesting suid binaries and the binary owner is root





11) find GTFO bins for suid method to perform privilege escalation

12) perform privilege escalation and we are root user now


nameless@nameless:~$ /usr/bin/id -a
/usr/bin/id: illegal option -- a
Usage: id [OPTION]... [USER]...
uid=2000(nameless) gid=1000(nameless) 3000(flag) groups=1000(nameless),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(lxd)
nameless