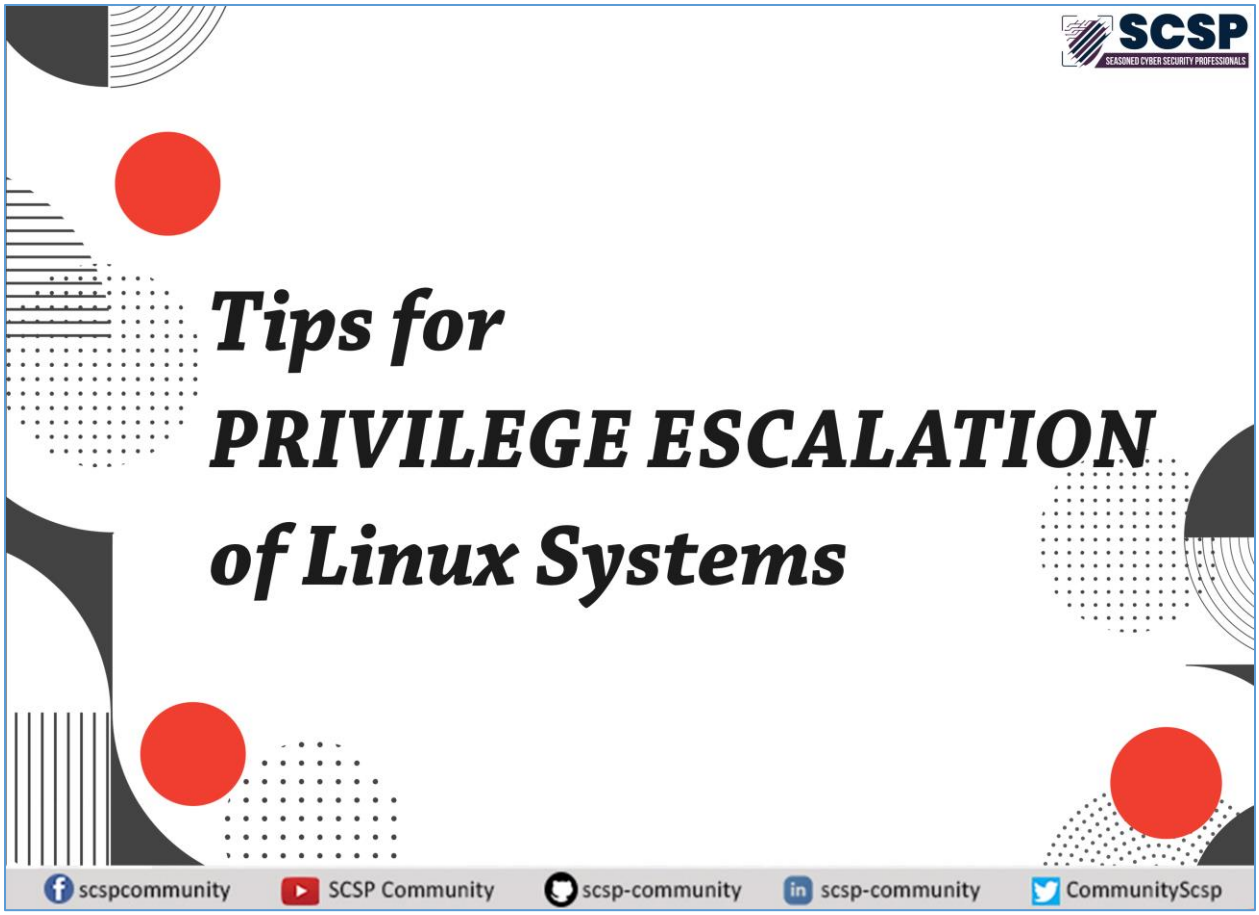
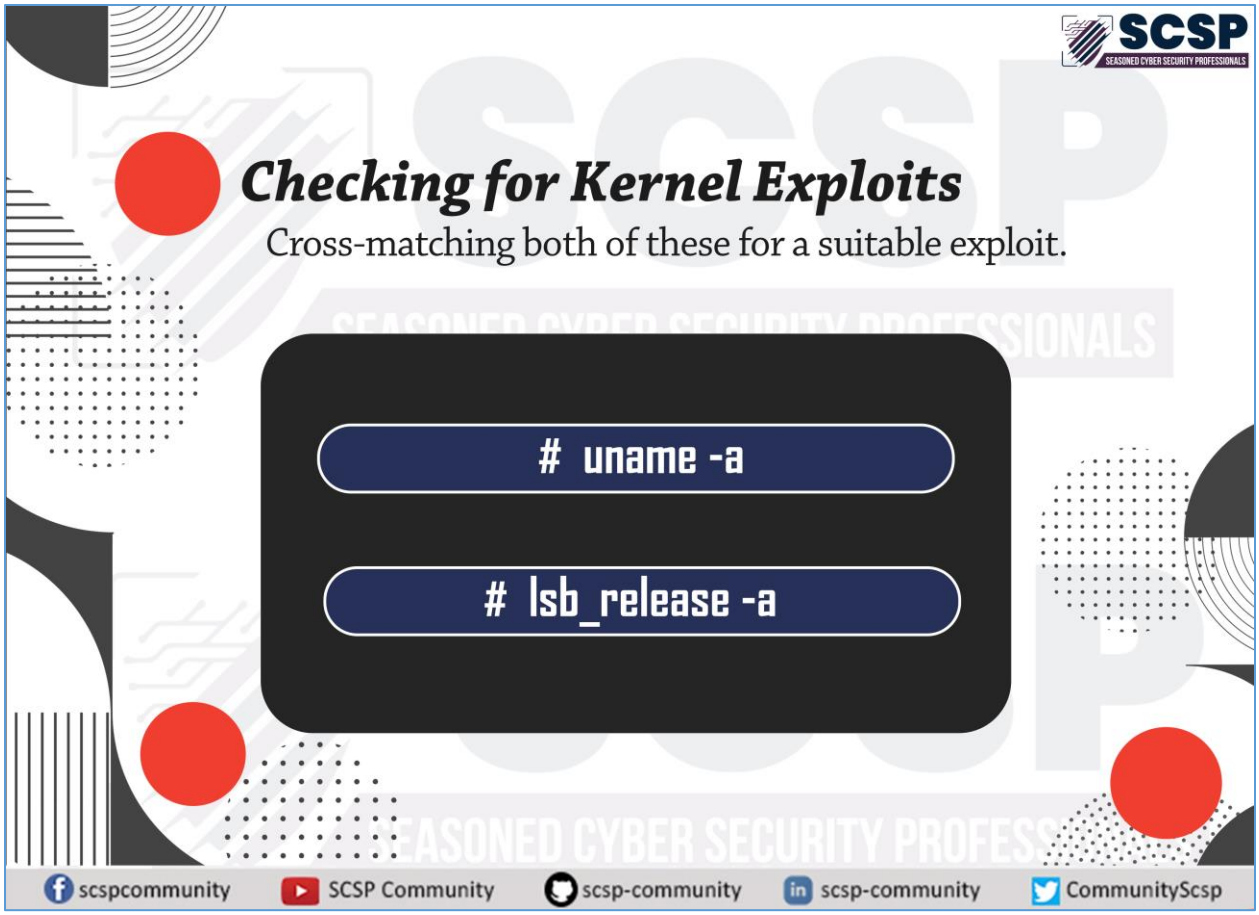
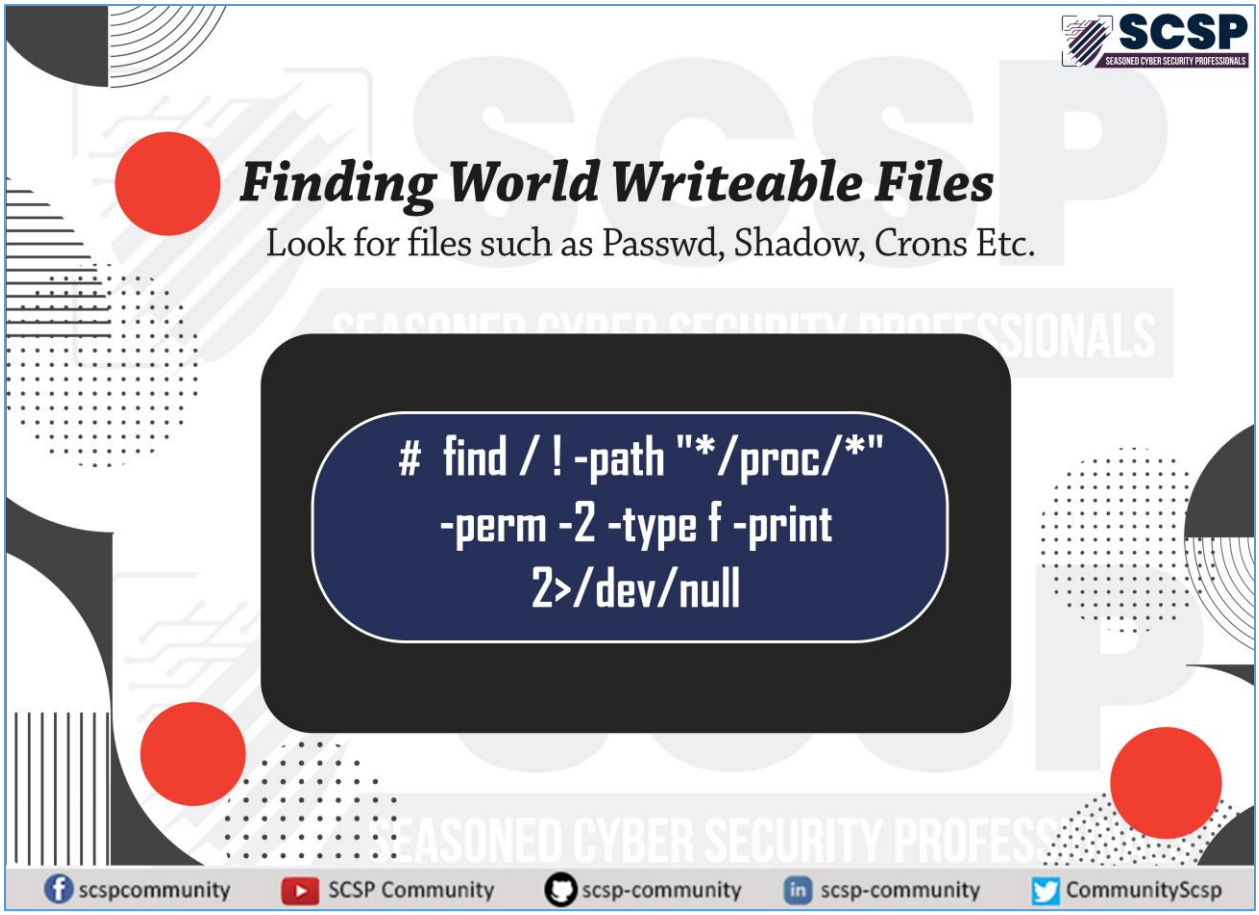
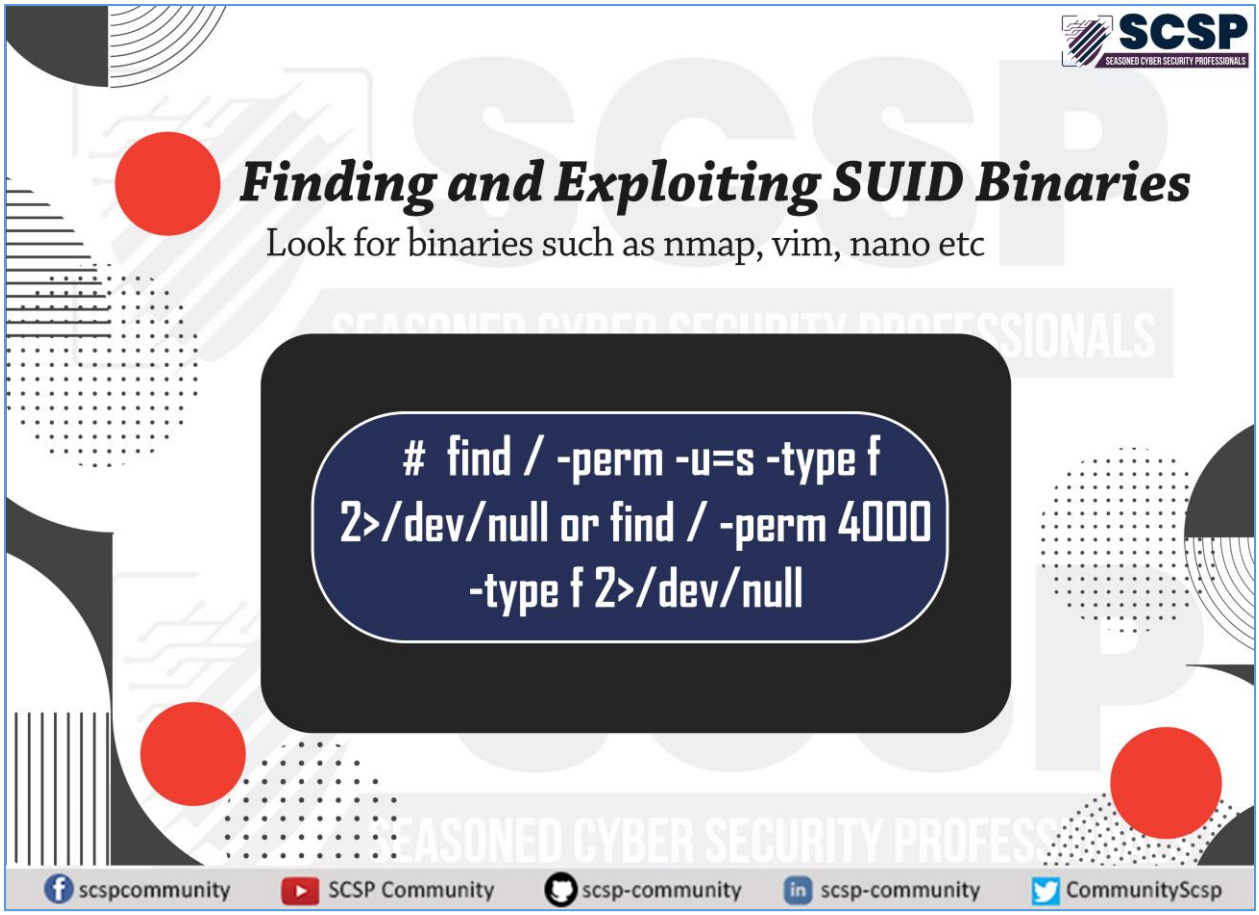
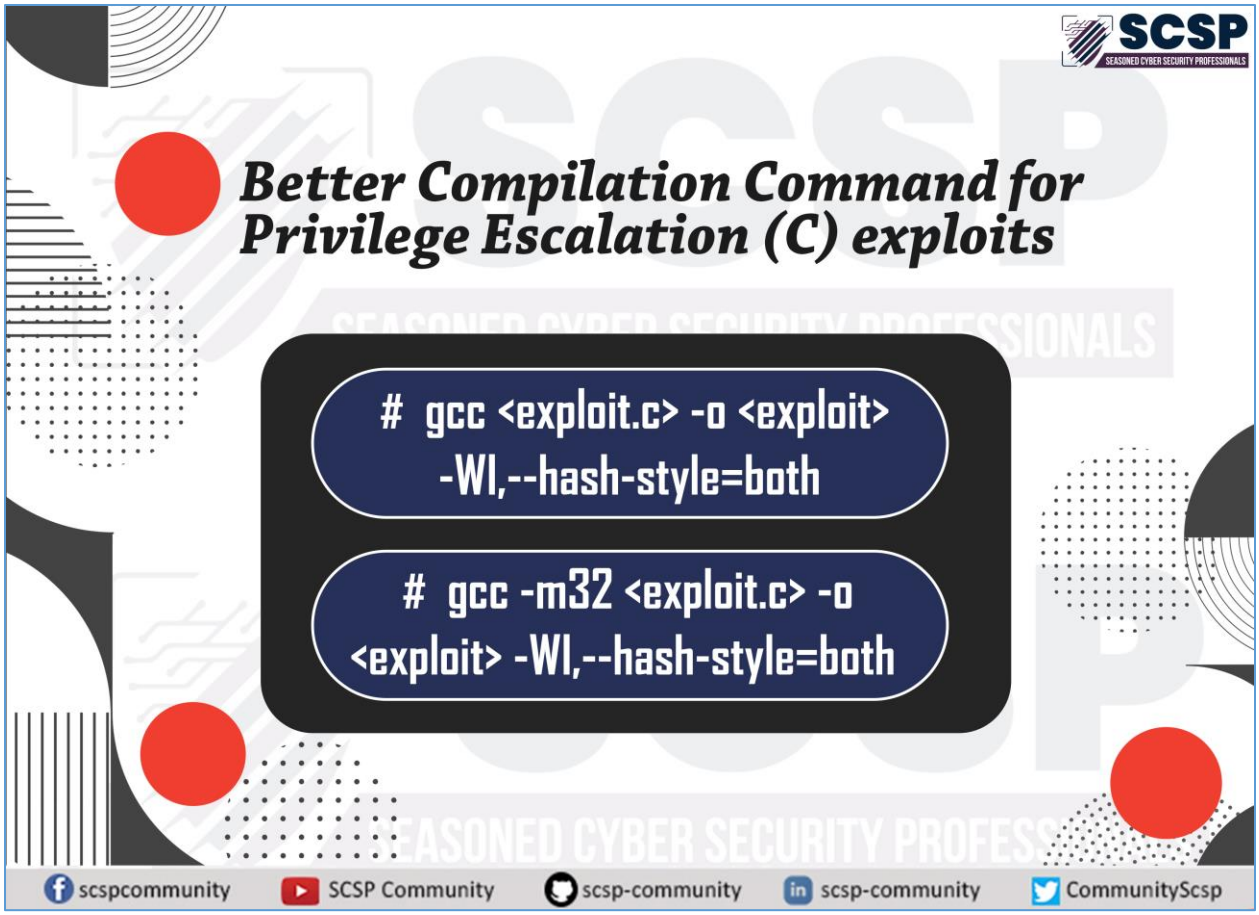

SCSP
SEASONED CYBER SECURITY PROFESSIONALS
Tips for
PRIVILEGE ESCALATION
of Linux Systems
scspcommunity
SCSP Community
scsp-community
scsp-community
CommunityScsp


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
Checking for Kernel Exploits
Cross-matching both of these for a suitable exploit.
uname -a
lsb_release -a
scspcommunity
SCSP Community
scsp-community
scsp-community
CommunityScsp


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
Finding World Writeable Files
Look for files such as Passwd, Shadow, Crons Etc.
find / ! -path "*/proc/*" -perm -2 -type f -print 2>/dev/null
scspcommunity
SCSP Community
scsp-community
scsp-community
CommunityScsp


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
Finding and Exploiting SUID Binaries
Look for binaries such as nmap, vim, nano etc
find / -perm -u=s -type f 2>/dev/null or find / -perm 4000 -type f 2>/dev/null
scspcommunity
SCSP Community
scsp-community
scsp-community
CommunityScsp


SCSP
SEASONED CYBER SECURITY PROFESSIONALS
Better Compilation Command for Privilege Escalation (C) exploits
gcc <exploit.c> -o <exploit> -Wl,--hash-style=both
gcc -m32 <exploit.c> -o <exploit> -Wl,--hash-style=both
scspcommunity
SCSP Community
scsp-community
scsp-community
CommunityScsp