TUTORIAL RED TEAM AREA (GENERAL)

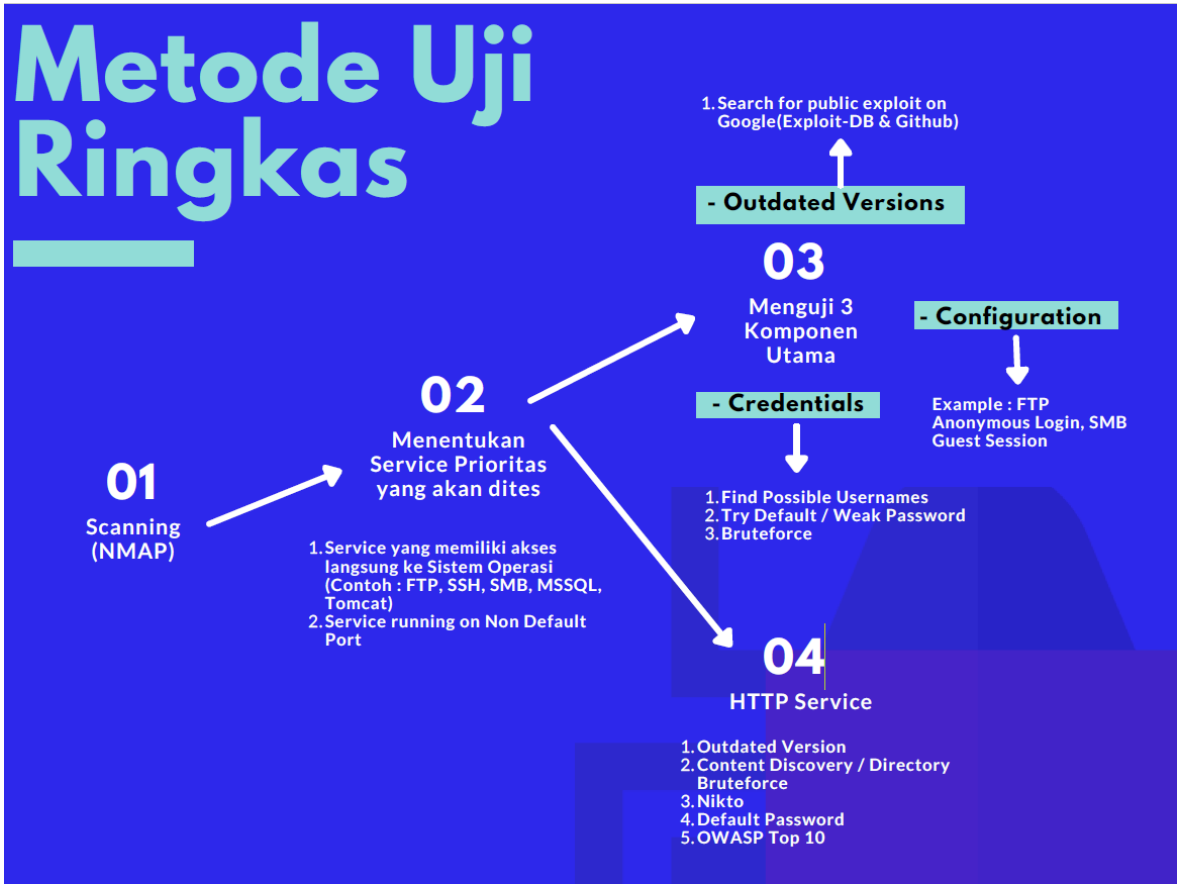
VA-PT Cheatsheet

Cheatsheet untuk Pentesting.

Catatan ini ditujukan untuk mempermudah pencarian payload/script tools dalam pentesting/VA.Cheatsheet ini disadur dari akun Github rekan saya Satrya Mahardhika ↗.

5 Tahap Ethical Hacking

Metode Uji Ringkas



NMAP Command

Berikut beberapa rangkuman perintah NMAP untuk tujuan *reconnaissance.* (Pindah dengan klik tab)

Best Practice | TCP Ports ... | TC... | UD... | Scan for vu...

```
nmap -sC -sV -p- -T4 Target IP
```

NMAP Command

#	Options	Description
1	-sT	TCP Connect port scan
2	-sU	UDP Port scan

3	-p	specific port scan
4	-p-	Scan All ports
5	-sV	Check Version of running service
6	-sC	Scan with default safe Scripts

#	Command	Scan For
1	nmap -sV `Target_IP`	Open TCP Ports and versions
2	nmap -sT `Target IP`	Open TCP Ports
3	nmap -sU `Target IP`	Open UDP Ports
4	nmap -sC -sV -p- `Target IP`	Open All TCP Ports and Versions + Scan with default NSE Scripts
5	nmap --vuln `Target IP`	Scan for vulnerability ()

Anda dapat mencari script NMAP pada:

```
ls /usr/share/nmap/scripts
```

Interesting Port

Port	Deskripsi	Port	Deskripsi
21	FTP server, unencrypted.	161, 162	SNMP Service
22	SSH server, can be connected to via SSH	389, 636	LDAP Directory Service
			HTTPS, check for HeartBleed? View

23	Telnet. Basically an unencrypted SSH	443	certificate for information?
25	SMTP - Email sending service.	445	SMB Shares service, likely vulnerable to an SMB RCE
69	TFTP Server. Very uncommon and old. Uses UDP.	587	Submission. If Postfix is run on it, it could be vunerable to shellshock
80	HTTP Server. Try visiting IP with web browser.	631	CUPS. Basically a Linux Printer Service for sharing printers.
88	Kerberos Service. Check, MS14-068 ↗	1433	Default MSSQL port. `sqsh -S 10.1.11.41 -U sa`
110	POP3 mail service. Login via telnet or SSH?	1521	Oracle DB. `tnscmd10g version -h 10.1.11.51`
111	RPCbind. This can help us look for NFS-shares	2021	Oracle XML DB. Check Default Passwords ↗
119	Network Time Protocol	2049	Network File System. `showmount -e 10.1.11.64`
135	MSRPC - Microsoft RPC	3306	MySQL Database. Connect: `mysql --host=10.1.11.69 -u root -p`
139	SMB Service. likely vulnerable to an SMB RCE	3389	Listening for RDP connection

Enumeration

SSH

Try connect to ssh service

```
ssh kali@10.131.2.128
```

FTP

Check for Anonymous login allowed. Use username: **anonymous ;** password: (blank or anything).(Pindah dengan klik tab)

Connect | Ambil File

```
ftp open Target_IP
```

SMB

Connect ke SMB untuk mengecek Shares yang available. (Pindah dengan klik tab)

Mencari share available | Connect

```
smbclient -L Target_IP
```

SMTP

Verify SMTP Port using netcat

```
nc -nv Target_IP 25
```

POP3

```
root@kali:~# telnet $ip 110
+OK beta POP3 server (JAMES POP3 Server 2.3.2) ready
USER billydean
+OK
PASS password
+OK Welcome billydean

list

+OK 2 1807
1 786
2 1021

retr 1

+OK Message follows
From: jamesbrown@motown.com
Dear Billy Dean,

Here is your login for remote desktop ... try not to forget it
this time!
username: billydean
password: PA$$W0RD!Z
```

WEB/ HTTP

1. Directory Finding

Directory finding adalah langkah penting dalam pemetaan situs web. Berikut beberapa tools yang bisa digunakan untuk melakukan directory brute forcing:

dirb

- **dirb** adalah alat untuk mencari direktori dan file di server web menggunakan wordlist.

  ```
  dirb http://<ip_target>/ /usr/share/wordlists/dirb/common.txt
  ```

- Anda bisa mengganti `common.txt` dengan wordlist lain yang lebih lengkap sesuai kebutuhan.

dirsearch

- **dirsearch** adalah tool Python yang lebih cepat dan mendukung multithreading dibandingkan dirb. Instalasi:

```
git clone https://github.com/maurosoria/dirsearch.git
cd dirsearch
pip install -r requirements.txt
```

- Penggunaan:

```
python3 dirsearch.py -u http://<ip_target>
```

2. Web Application Scanning

Untuk memeriksa potensi kerentanannya, Anda bisa melakukan pemindaian aplikasi web dengan tools berikut:

Nikto

- **Nikto** adalah scanner web server yang mencari lebih dari 6700 potensi masalah keamanan.

```
nikto -h http://<ip_target>
```

Nuclei (Pemindaian Kerentanannya)

- **Nuclei** adalah framework pemindaian kerentanannya yang sangat cepat. Nuclei dapat digunakan untuk memindai berbagai jenis kerentanannya seperti CVE, XSS, SQLi, dan lainnya. Instalasi:

```
sudo apt install nuclei
```

- Penggunaan dasar:

```
nuclei -u http://<ip_target>
```

- Anda bisa menggunakan template lain untuk pemindaian lebih mendalam, misalnya XSS:

```
nuclei -u http://<ip_target> -t xss/
```

3. CMS Scanning

Jika situs web menggunakan CMS tertentu, Anda bisa menggunakan tools khusus untuk memeriksa kerentanannya. Beberapa CMS umum dan tools yang dapat digunakan adalah:

WordPress (WPScan)

WPScan adalah alat populer untuk memindai kerentanannya di situs WordPress.

- **Pemasangan WPScan:**

  ```
  sudo apt install wpscan
  ```

- **Pemindaian Dasar:**

  ```
  wpscan --url http://<ip_target>
  ```

- **Pemindaian API (memerlukan API key):** Untuk pemindaian lebih mendalam, gunakan API WPScan dengan API Key yang bisa didapatkan di situs resmi WPScan:

  ```
  wpscan --api-token <YOUR_API_KEY> --url http://<ip_target>
  ```

- **Pemeriksaan Plugin Agresif:** Untuk memeriksa plugin yang terpasang dengan cara agresif:

  ```
  wpscan --url http://<ip_target> -e ap --plugins-detection
  aggressive
  ```

Joomla (Joomscan)

Untuk memindai Joomla, Anda dapat menggunakan **Joomscan**.

- **Instalasi:**

  ```
  git clone https://github.com/rezasp/joomscan.git
  cd joomscan
  chmod +x joomscan.py
  ```

- **Pemindaian:**

```
python joomscan.py -u http://<ip_target>
```

Drupal (Droopescan)

Untuk memindai kerentanannya di situs Drupal, gunakan **Droopescan**.

- **Instalasi:**

```
git clone https://github.com/droope/droopescan.git
cd droopescan
python3 setup.py install
```

- **Pemindaian:**

```
droopescan scan drupal -u http://<ip_target>
```

Magento (MageScan)

Untuk Magento, gunakan **MageScan**.

- **Instalasi:**

```
git clone https://github.com/MagentoHackers/magescan.git
cd magescan
chmod +x magescan.py
```

- **Pemindaian:**

```
python magescan.py http://<ip_target>
```

Mencari Exploit

Melalui Mesin Pencari (Google)

1. Perhatikan dan cari versi aplikasi yang kemungkinan rawan.
2. Lakukan pencarian di mesin pencari dengan format "[APLIKASI] [VERSI] [EXPLOIT]" . Contoh: "Samba 3.5.0 exploit"
3. Prioritaskan sumber dari ExploitDB / Github /Rapid7.
4. Unduh dan gunakan exploit sesuat keterangan pada sumber terkait.

Melalui Searchploit (Kali)

```
searchsploit linux 2.2.0
#Mencari exploit dengan keyword tertentu contoh linux 2.2.0
#Mendownload (Copy) exploit ke working directory

searchsploit -m Nomor_Exploit

wget Alamat_URL
#Download File
```

Bruteforce/Hash Cracking (sample)

SSH Bruteforce With Hydra

```
hydra -L users.txt -P pass.txt 192.168.1.181 ssh
```

John The Ripper common hash

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash
```

Hashcat crack md5

```
hashcat -m 13100 hash.txt /usr/share/wordlists/rockyou.txt --
outfile=cracked.txt
```

Command Execution Guide

Reverse Shell

(Pindah dengan klik tab)

(LISTENER) YANG DI ATTACKER	YANG DI KIRIM KE VICTIM(TARGET)

```
nc -nlvp 4444
```

Sumber lain untuk membuat reverse shell disini ↗ .

Upgrade ke Interactive Shell

```
python -c 'import pty;pty.spawn("/bin/bash")'
CTRL+Z
stty raw -echo; fg
<ENTER>
<ENTER>
```

Sumber lain untuk interactive shell dapat dicek di Linux TTY Shell Cheat Sheet

Previous
Linux Command Intro

Next
Penetration Testing Guide & Checklist