

# TUGAS INDIVIDU 1: MENGIDENTIFIKASI SERANGAN- SERANGAN SIBER PADA WEB APPLICATION

*Nama = Damelia*

*NIM = 1803421013*

*Kelas = BM 6A*



Keamanan dan Keandalan Jaringan  
Politeknik Negeri Jakarta

## Bagian 1. Social Engineering

Tujuan: Mahasiswa dapat menjelaskan Teknik-teknik yang digunakan untuk gaining privileges dengan social engineering.

Tuliskan apa yang anda ketahui tentang social engineering dan Teknik-tekniknya dalam serangan social engineering? Minimal ditulis dalam 1 paragraf dengan 1 contoh Teknik serangan social engineering. (contoh: phishing lewat link email, dll)

### Jawab:

Yang saya ketahui mengenai social engineering adalah suatu teknik untuk menipu/memanipulasi korban dengan cara memanfaatkan sisi kelemahan manusia sebagai makhluk biologis yang mempunyai perasaan dan emosi. Penyerang akan mengendalikan emosi, ketakutan si korban, dan memojokannya agar segera melakukan hal yang diinginkan penyerang. Seperti membuka link, membuka file, melakukan update, mentransfer uang, dan lain-lainnya.

Keberhasilan dalam social engineering sangat tergantung pada kemampuan penyerang untuk memanipulasi pikiran korban, kegiatan ini tidak hanya dilakukan di dunia maya (online) namun bisa juga terjadi melalui tatap muka. Maka dari itu, social engineering merupakan ancaman terbesar bagi individu maupun organisasi saat ini karena manusia sangat rentan dalam melakukan tindakan ceroboh saat dirinya diberi tekanan emosi dan perasaan.

Contoh serangan social engineering sangat banyak sekali, namun disini saya akan menjelaskannya berdasarkan pengalaman pribadi keluarga saya dan film-film yang saya tonton.

#### (1) Baiting

Baiting merupakan serangan dalam social engineering online dan fisik yang menjanjikan korban sebuah hadiah. Pada saat saya berumur 12 tahun, Ibu saya mendapatkan voucher pemenang undian berhadiah mobil dari bungkus pop mie. Pada saat itu di tv sedang viral tentang iklan pop mie tersebut yang bisa membuat pelanggannya mendapatkan mobil secara cuma-cuma.

Kemudian Ibu saya bergegas menghubungi pihak yang tertera pada voucher tersebut dan mendapatkan jawaban panggilan. Pihak pop mie mengatakan jika ingin mendapatkan mobilnya harus mentransfer pulsa sebanyak 100 ribu dahulu sebagai persyaratan surat-surat mobil. Dikarenakan Ibu saya sangat menginginkan mobil tersebut, ditransfer lah pulsa 100 ribu itu.

Setelah di transfer pihak pop mie meminta lagi yaitu uang sebesar 200 ribu untuk biaya pengiriman dan Ibu saya menyetujuinya. Pada saat itu sudah 300 ribu uang yang diterima pihak pop mie dari Ibu saya. Dengan uang yang sudah ditransfer tersebut harusnya mobil akan segera datang, namun yang terjadi selalu ada penundaan. Lalu pihak pop mie mendesak Ibu saya dan menghubunginya terus-menerus untuk transfer lagi sebesar 500 ribu dengan rayuan dan tipuan untuk memanipulasi pikiran Ibu saya. Disitu Ibu saya sangat bimbang dan sadar bahwa selama ini ia ditipu, kemudian memutuskan mengakhiri keinginannya untuk mendapatkan mobil tersebut. Serangan social engineering ini memberi pelajaran bagi keluarga saya untuk tidak mempercayai undian orang tidak dikenal apalagi mentransfer uang.

## (2) Phishing

Phishing adalah taktik manipulasi dan penipuan melalui email, situs web, dan pesan teks untuk mencuri informasi. Saya sangat suka menonton film, apalagi film yang bertema hacker. Salah satunya adalah film "Who Am I". Pada film ini ada sebuah adegan serangan phishing yang dilakukan Clay, kelompok hacker beranggotakan 4 orang yang menjadi pemeran utama pada film ini. Pada adegan tersebut Clay ingin meretas dinas rahasia Jerman yaitu Bundesnachrichtendienst (BND).

Mereka masuk ke tempat pembuangan sampah sisa perkantoran seperti kertas-kertas di BND untuk mencari dan mendapatkan informasi. Kemudian mereka mendapatkan diary salah satu karyawan BND yang bernama Gerdi, isi diary itu adalah curhatan tentang kecintaannya terhadap kucing. Dari informasi diary tersebut Clay mengirimkan email yang berpura-pura menjadi salah satu pet shop bernama "Sabine" (pet shop favorit Gerdi) dan meminta Gerdi untuk membuka link yang ada di email tersebut jika ia ingin melihat anak kucing lucu. Pada saat itu Gerdi tergoda dan sangat ingin melihat anak kucing lucu. Setelah Gerdi membuka linknya, Clay langsung meretas pc milik Gerdi. Melalui pc Gerdi, Clay bisa mendapatkan akses ke jaringan di BND yang akhirnya Clay dapat meretas server BND.

Dari adegan tersebut saya dapat memahami teknik phishing melalui email dengan memanipulasi emosi melalui hobby korban sehingga korban mendapatkan kepercayaan dan penyerang dapat mencuri data, informasi, dan lain-lain.

## Bagian 2. Cyber Kill Chain

**Tujuan:** Mahasiswa dapat menjelaskan tahapan-tahapan yang dilakukan hacker dalam menjalankan aksi dengan tujuan untuk mencapai kerusakan pada target atau Zero Day.

Deskripsikan apa yang anda ketahui tentang Cyber Kill Chain?

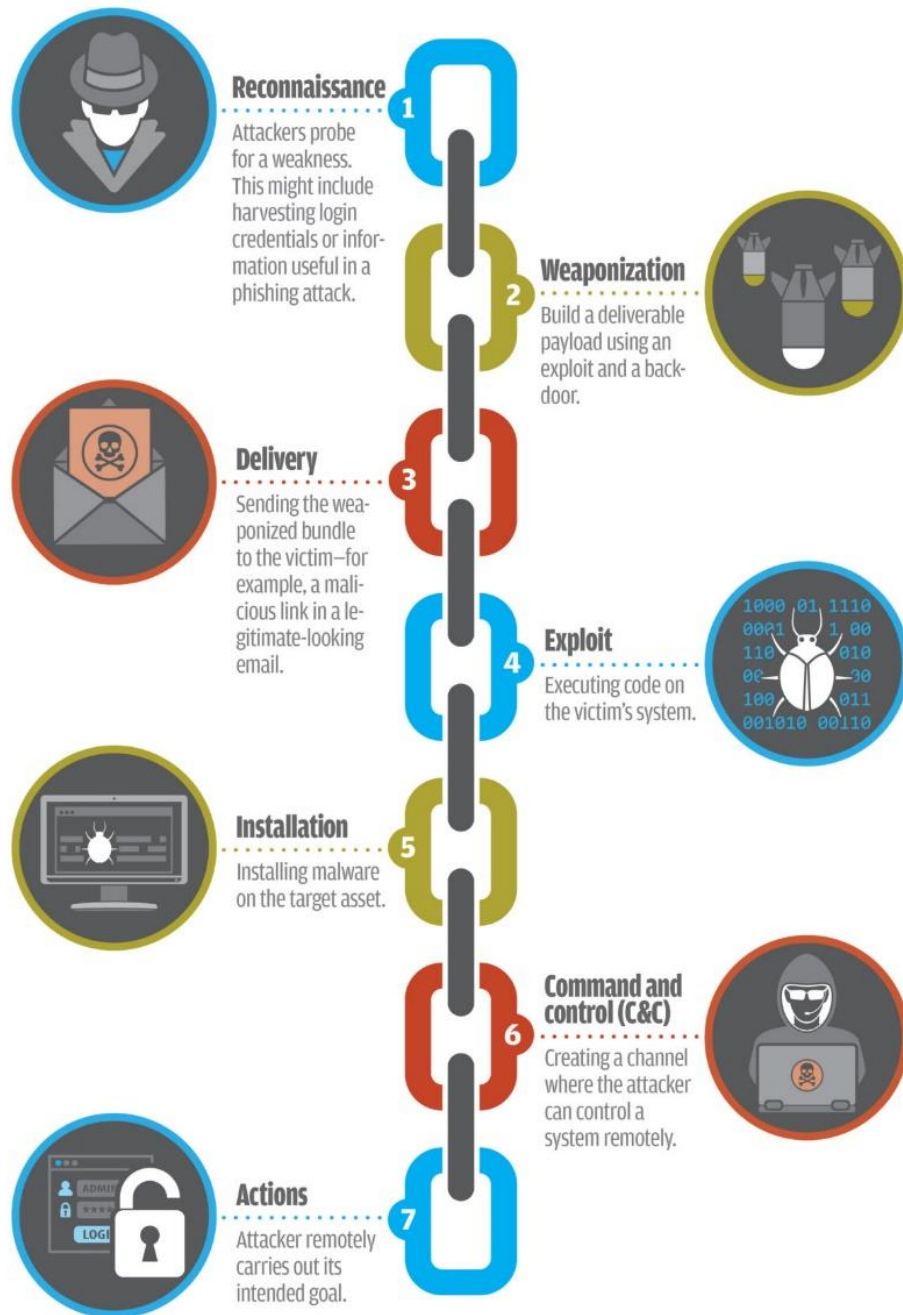
Boleh disertai dengan gambar diagram. Dan tahapan mana yang digunakan seorang hacker untuk mengambil informasi-informasi awal mengenai targetnya? Jelaskan tahapan tersebut.

### **Jawab:**

Yang saya ketahui Cyber Kill Chain merupakan urutan tahapan-tahapan yang dilakukan penyerang dalam menjalankan aksinya agar berhasil menyusup dan meretas jaringan dengan tujuan untuk mencapai kerusakan pada target (zero day).

# What is the **CYBER KILL CHAIN**?

The cyber kill chain, created by Lockheed Martin, describes the phases or stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack.



SOURCE: LOCKHEED MARTIN

Gambar Diagram Cyber Kill Chain

Penjelasan masing-masing tahapan:

### **(1) Reconnaissance**

Reconnaissance adalah kegiatan seorang penyerang (hacker) mencoba memutuskan apa yang menjadi (dan bukan) target yang baik dan juga mendapatkan informasi sebanyak mungkin tentang jaringan targetnya sebelum meluncurkan jenis serangan lain yang lebih serius. Seringkali, reconnaissance dilaksanakan dengan menggunakan informasi yang tersedia.

Tujuan reconnaissance adalah penyerang akan fokus pada target yang kemungkinan besarnya memiliki hak istimewa (baik untuk akses sistem atau akses ke data rahasia). Penyerang akan menggali informasi mengenai targetnya seperti arsitektur dan tata letak jaringan, alat, perangkat, protokol dan infrastruktur kritis. Ini seperti perampok memahami perilaku korban dan membobol rumah korban.

Jenis reconnaissance ada 2 yaitu:

- **Passive reconnaissance**  
Seorang hacker mencari informasi yang tidak berhubungan dengan domain korban. Dia hanya mengetahui domain terdaftar ke sistem target sehingga dia dapat menggunakan perintah (misalnya direktori telepon) untuk mendapatkan informasi tentang target.
- **Active reconnaissance**  
Seorang hacker menggunakan informasi sistem untuk mendapatkan akses tidak sah ke materi digital atau elektronik yang dilindungi dan mungkin menjelajahi router atau bahkan firewall untuk mendapatkannya.

### **(2) Weaponization**

Pada tahap weaponization para penyerang membuat tools untuk menyerang target pilihan mereka dengan menggunakan informasi yang telah mereka kumpulkan dan menggunakannya untuk suatu tujuan yang jahat. Semakin banyak informasi yang dapat mereka gunakan, semakin kuat serangan manipulasi psikologis.

Tools yang terkenal digunakan oleh para penyerang adalah:

- **Botnet**  
Jaringan komputer yang dipaksa untuk bekerja sama atas perintah pengguna jarak jauh yang tidak sah. Jaringan komputer robot ini digunakan untuk menyerang sistem lain.
- **DDOS**  
Serangan Distributed Denial of Service adalah saat sistem atau jaringan komputer dibanjiri dengan lalu lintas data, sehingga sistem tidak dapat menangani volume permintaan dan sistem atau jaringan dimatikan.
- **Malware**  
Malicious software adalah perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya. Contohnya: Logic bomb, worm, virus, packet sniffer (menguping di jaringan).

### (3) Delivery

Pada tahap delivery penyerang mengirimkan payload berbahaya ke target seperti email, yang merupakan salah satu dari banyak metode penyusupan yang dapat digunakan penyerang. Ada lebih dari 100 metode delivery yang memungkinkan.

Terdapat dua metode dasar pada delivery:

- Adversary-controlled delivery, yang melibatkan peretasan langsung ke port terbuka.
- Adversary-released delivery, yang menyampaikan malware ke target melalui phishing.

### (4) Exploitation

Setelah penyerang mengidentifikasi vulnerability di sistem target, mereka mengeksploitasi kelemahan tersebut dan melakukan serangan mereka. Selama fase exploitation, host machine akan disusupi oleh penyerang dan mekanisme delivery biasanya akan mengambil salah satu dari dua tindakan:

- Install malware (a dropper), yang memungkinkan eksekusi perintah penyerang.
- Install malware (a downloader) dan download malware tambahan dari Internet, yang memungkinkan eksekusi perintah penyerang.

Setelah foothold dibuat di dalam jaringan, penyerang biasanya akan mengunduh tools tambahan, mencoba eskalasi hak istimewa, mengekstrak hash kata sandi, dll.

### (5) Installation

Pada tahap installation ini, malware menginstal jalur akses untuk penyerang (backdoor). Malware dapat berupa ransomware, remote-access Trojans, atau aplikasi lain yang tidak diinginkan. Installation (pemasangan) backdoor pada sistem komputer yang disusupi memungkinkan musuh melewati kontrol keamanan dan mempertahankan akses di lingkungan korban.

### (6) Command and Control

Pada tahap command and control ini, malware memberikan akses penyerang pada sistem. Ransomware menggunakan koneksi perintah dan kontrol untuk mengunduh kunci enkripsi sebelum membajak file target. Contohnya, remote-access Trojans membuka perintah koneksi kontrol untuk memungkinkan akses jarak jauh ke sistem target.

Command and control sumber daya yang disusupi biasanya dilakukan melalui suar melalui jalur yang diizinkan keluar dari jaringan. Beacons memiliki banyak bentuk, tetapi dalam banyak kasus cenderung:

- Berbasis HTTP atau HTTPS
- Dibuat agar terlihat seperti lalu lintas biasa melalui header HTTP yang dipalsukan

Dalam kasus yang menggunakan komunikasi terenkripsi, suar cenderung menggunakan sertifikat yang ditandatangani sendiri atau menggunakan enkripsi khusus melalui jalur yang diizinkan.

### (7) Actions

Action mengacu bagaimana penyerang mencapai tujuan akhirnya. Tujuan akhir penyerang dapat berupa apa saja, seperti enkripsi untuk tebusan, eksfiltrasi data, atau bahkan penghancuran data.

### Bagian 3. Web Vulnerabilities

Tujuan: Mahasiswa dapat menjelaskan bagaimana Teknik reconnaissance yang dilakukan hacker untuk gaining informasi awal mengenai target.

Buka web berikut: <https://www.ceos3c.com/security/scan-for-website-vulnerabilities-with-nikto/>

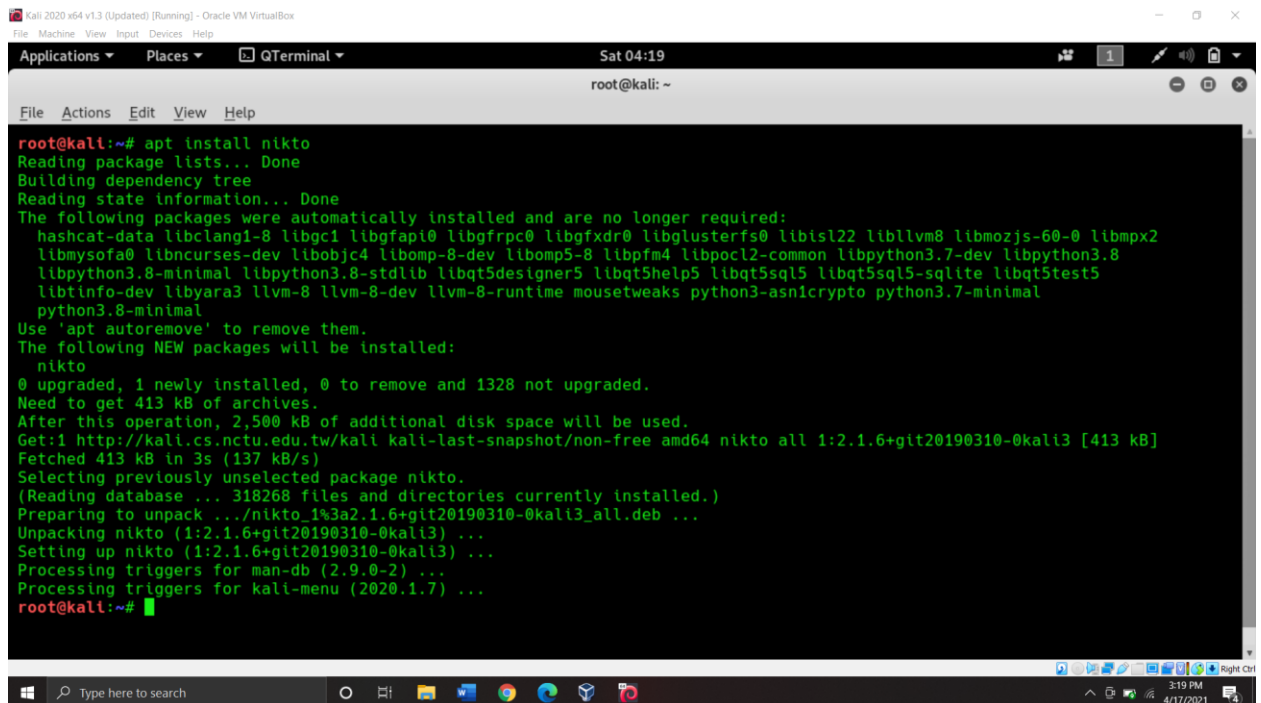
Dan lakukan tahapan instalasi yang ada di web tersebut.

Kemudian lakukan scan pada web yang vulnerable berikut ini: <http://www.itsecgames.com/>

Pertanyaan: Jelaskan yang terjadi pada saat anda menjalankan command nikto -h <server-address> -p 80

**Jawab:**

(1) Pertama saya install nikto → `apt install nikto`



```
Kali 2020 x64 v1.3 (Updated) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places QTerminal Sat 04:19
root@kali: ~
File Actions Edit View Help

root@kali:~# apt install nikto
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  hashcat-data libclang1-8 libgc1 libgelf0 libgfrpc0 libgfxdr0 libglusterfs0 libisl22 libllvm8 libmozjs-60-0 libmpx2
  libmysofa0 libncurses-dev libobjc4 libomp-8-dev libomp5-8 libpfm4 libpoc12-common libpython3.7-dev libpython3.8
  libpython3.8-minimal libpython3.8-stdlib libqt5designer5 libqt5help5 libqt5sql5 libqt5sql5-sqlite libqt5test5
  libtinfo-dev libyara3 llvm-8 llvm-8-dev llvm-8-runtime mousetweaks python3-asn1crypto python3.7-minimal
  python3.8-minimal
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  nikto
0 upgraded, 1 newly installed, 0 to remove and 1328 not upgraded.
Need to get 413 kB of archives.
After this operation, 2,500 kB of additional disk space will be used.
Get:1 http://kali.cs.nctu.edu.tw/kali kali-last-snapshot/non-free amd64 nikto all 1:2.1.6+git20190310-0kali3 [413 kB]
Fetched 413 kB in 3s (137 kB/s)
Selecting previously unselected package nikto.
(Reading database ... 318268 files and directories currently installed.)
Preparing to unpack .../nikto_1%3a2.1.6+git20190310-0kali3_all.deb ...
Unpacking nikto (1:2.1.6+git20190310-0kali3) ...
Setting up nikto (1:2.1.6+git20190310-0kali3) ...
Processing triggers for man-db (2.9.0-2) ...
Processing triggers for kali-menu (2020.1.7) ...
root@kali:~#
```

(2) Download → `wget https://github.com/sullo/nikto/archive/master.zip`  
Lalu, Ekstrak file → `unzip master.zip`

```
Kali 2020 v64 v1.3 (Updated) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Applications ▾ Places ▾ QTerminal ▾ Sat 04:30
root@kali: ~

File Actions Edit View Help

root@kali:~# wget https://github.com/sullo/nikto/archive/master.zip
--2021-04-17 04:25:22-- https://github.com/sullo/nikto/archive/master.zip
Resolving github.com (github.com)... 192.30.255.112
Connecting to github.com (github.com)|192.30.255.112|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/sullo/nikto/zip/master [following]
--2021-04-17 04:25:31-- https://codeload.github.com/sullo/nikto/zip/master
Resolving codeload.github.com (codeload.github.com)... 192.30.255.120
Connecting to codeload.github.com (codeload.github.com)|192.30.255.120|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 510740 (499K) [application/zip]
Saving to: 'master.zip'

master.zip                               100%[=====] 498.77K  96.9KB/s   in 5.1s

2021-04-17 04:25:38 (96.9 KB/s) - 'master.zip' saved [510740/510740]

root@kali:~# unzip master.zip
Archive:  master.zip
d27173173bebac29fa89ef3a493febab16594a12
  creating: nikto-master/
  inflating: nikto-master/.dockerignore
  inflating: nikto-master/.editorconfig
  extracting: nikto-master/.gitattributes
  creating: nikto-master/.github/
  extracting: nikto-master/.github/FUNDING.yml
  creating: nikto-master/.github/ISSUE_TEMPLATE/
```

(3) Masuk ke file nikto → cd nikto-master/program  
→ perl nikto.pl

```
Kali 2020 v64 v1.3 (Updated) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Applications ▾ Places ▾ QTerminal ▾ Sat 04:34
root@kali: ~/nikto-master/program

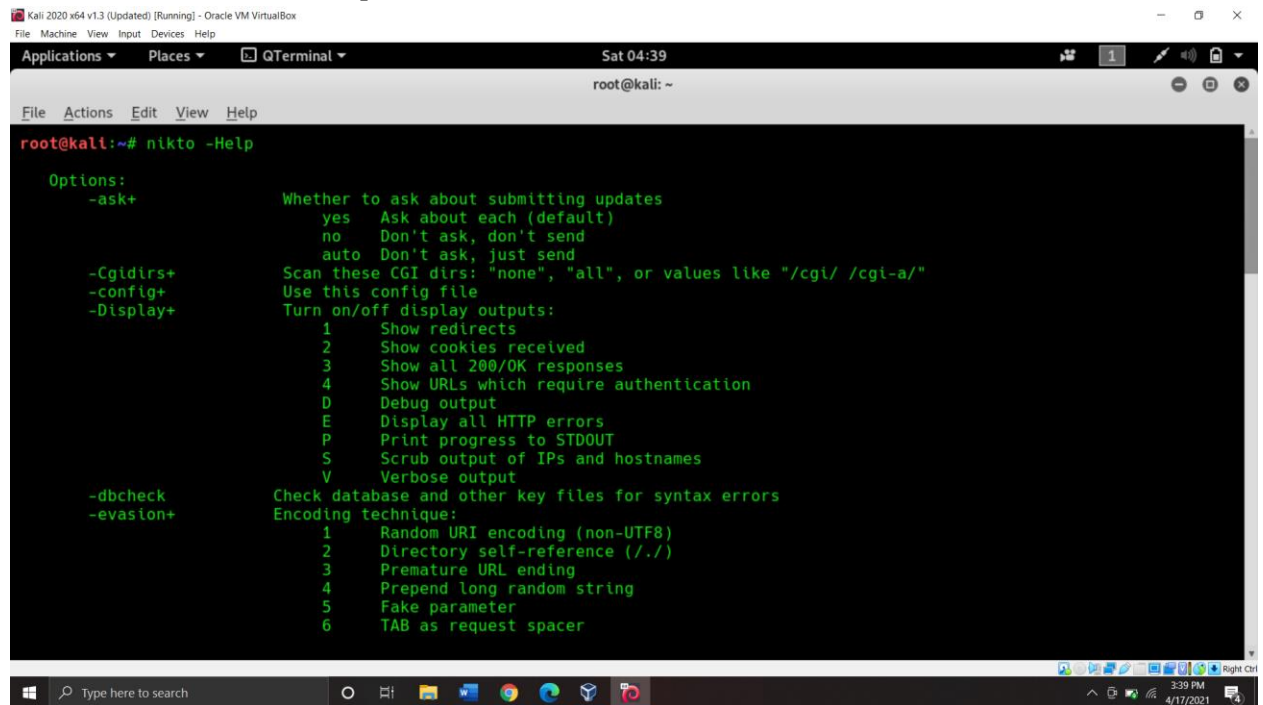
File Actions Edit View Help

root@kali:~# cd nikto-master/program
root@kali:~/nikto-master/program# perl nikto.pl
- Nikto v2.1.6
-----
+ ERROR: No host (-host) specified

  -config+      Use this config file
  -Display+     Turn on/off display outputs
  -dbcheck+     check database and other key files for syntax errors
  -Format+      save file (-o) format
  -Help+        Extended help information
  -host+        target host/URL
  -id+          Host authentication to use, format is id:pass or id:pass:realm
  -list-plugins List all available plugins
  -output+      Write output to this file
  -nossL        Disables using SSL
  -no404+       Disables 404 checks
  -Plugins+     List of plugins to run (default: ALL)
  -port+        Port to use (default 80)
  -root+        Prepend root value to all requests, format is /directory
  -ssl+         Force ssl mode on port
  -Tuning+      Scan tuning
  -timeout+     Timeout for requests (default 10 seconds)
  -update+      Update databases and plugins from CIRT.net
  -Version+     Print plugin and database versions
  -vhost+       Virtual host (for Host header)
               + requires a value
```



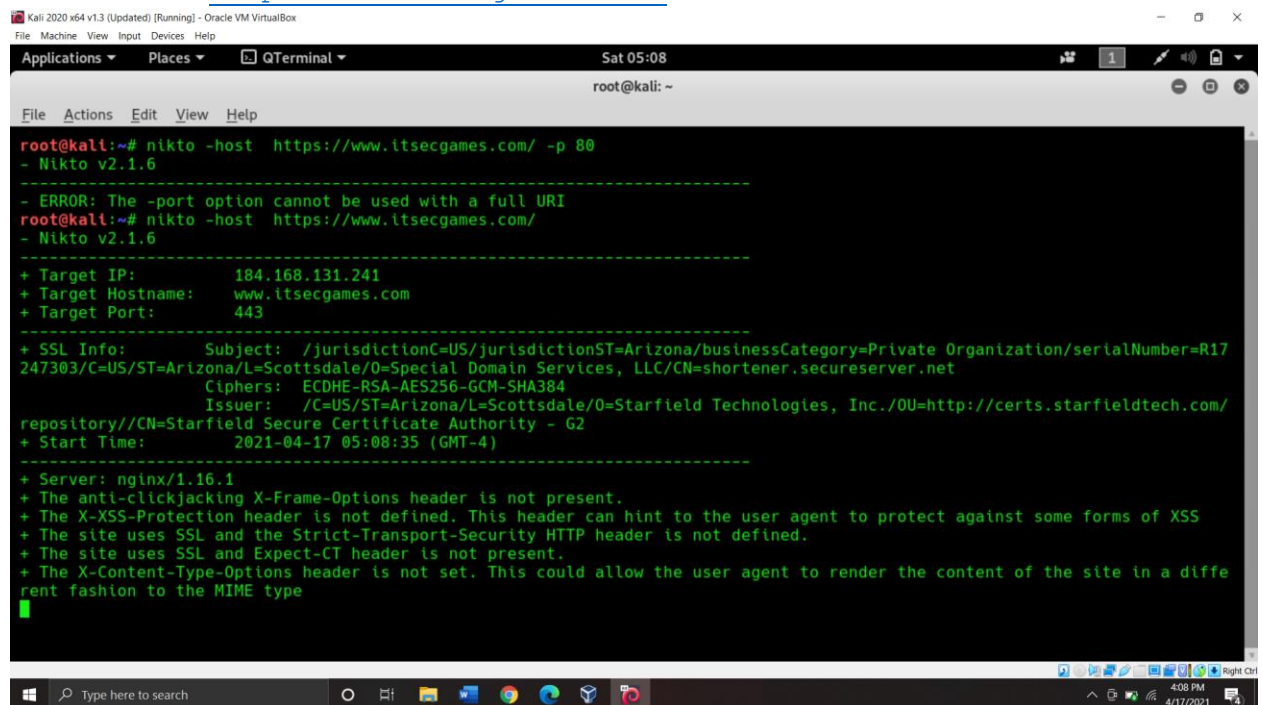
(4) Mencoba nikto → `nikto -Help`



```
root@kali:~# nikto -Help

Options:
-ask+          Whether to ask about submitting updates
                yes   Ask about each (default)
                no   Don't ask, don't send
                auto  Don't ask, just send
-Cgldirs+      Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
-config+       Use this config file
-Display+      Turn on/off display outputs:
                1   Show redirects
                2   Show cookies received
                3   Show all 200/OK responses
                4   Show URLs which require authentication
                D   Debug output
                E   Display all HTTP errors
                P   Print progress to STDOUT
                S   Scrub output of IPs and hostnames
                V   Verbose output
-dbcheck       Check database and other key files for syntax errors
-evasion+      Encoding technique:
                1   Random URI encoding (non-UTF8)
                2   Directory self-reference (../)
                3   Premature URL ending
                4   Prepend long random string
                5   Fake parameter
                6   TAB as request spacer
```

(5) Scan web: <http://www.itsecgames.com/>  
→ `nikto -host http://www.itsecgames.com/`



```
root@kali:~# nikto -host https://www.itsecgames.com/ -p 80
- Nikto v2.1.6
-----
- ERROR: The -port option cannot be used with a full URI
root@kali:~# nikto -host https://www.itsecgames.com/
- Nikto v2.1.6
-----
+ Target IP:      184.168.131.241
+ Target Hostname: www.itsecgames.com
+ Target Port:    443
-----
+ SSL Info:      Subject:  /jurisdictionC=US/jurisdictionST=Arizona/businessCategory=Private Organization/serialNumber=R17
247303/C=US/ST=Arizona/L=Scottsdale/O=Special Domain Services, LLC/CN=shortener.secureserver.net
Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
Issuer:    /C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./OU=http://certs.starfieldtech.com/
repository//CN=Starfield Secure Certificate Authority - G2
+ Start Time:    2021-04-17 05:08:35 (GMT-4)
-----
+ Server: nginx/1.16.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diffe
rent fashion to the MIME type
```

(6) Penjelasan hasil:

Pada saat saya melakukan scan menggunakan perintah `nikto -host http://www.itsecgames.com/ -p 80` hasil yang didapatkan adalah ERROR: The -port option cannot be used with a full URI.

Kemudian perintahnya saya ubah dengan tidak menulis portnya menjadi `nikto -host http://www.itsecgames.com/` dan hasil yang didapatkan seperti gambar diatas. Terdapat alamat IP target, nama host target, port target, informasi web server yaitu nginx/1.16.1, web tersebut menggunakan SSL, dan informasi tentang vulnerabilities lainnya.

#### Bagian 4. Distributed Denial of Service

**Tujuan:** Mahasiswa dapat menjelaskan bagaimana serangan DDoS dapat melumpuhkan layanan target web aplikasi.

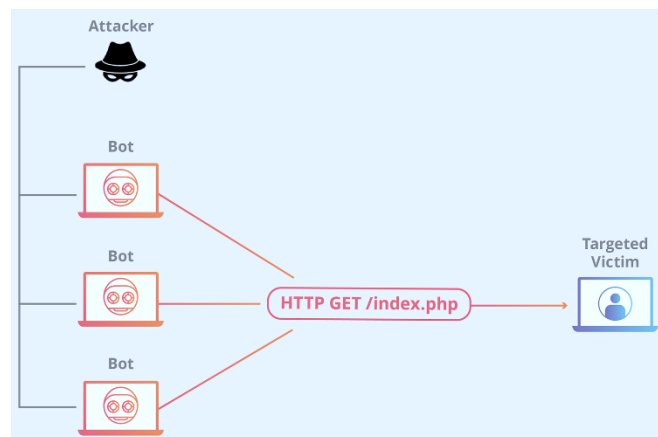
Tuliskan apa yang anda ketahui tentang DDoS? Jelaskan bagaimana prosesnya teknik serangan ini untuk melumpuhkan Aplikasi Web? Dan apa yang terjadi pada target Aplikasi ketika DDoS ini dilakukan?

**Jawab:**

DDoS (Distributed Denial of Service) adalah teknik serangan dengan cara membuat server atau sumber daya target berjalan dengan beban yang berat (overload) sampai tidak bisa lagi menampung koneksi dari user lain dengan mengirimkan request ke server secara terus menerus dengan transaksi data yang besar. Serangan ini dilakukan menggunakan beberapa komputer host penyerang sampai dengan komputer target tidak bisa diakses.

Berikut proses DDoS ini untuk melumpuhkan Aplikasi Web:

- (1) Penyerang memerlukan botnet untuk menjalankan aksi DDoS. Botnet adalah komputer atau jaringan yang diretas, kemudian dikendalikan secara remote oleh hacker pada DDoS. Botnets inilah mesin yang digunakan pelaku untuk membanjiri traffic. Perangkat Internet of Thing (IoT) seperti smart tv, kamera digital, printer, smartphone, kamera, juga bisa dieksploitasi menjadi botnet. Perangkat-perangkat tersebut biasanya memiliki sistem keamanan yang lebih rentan dibanding komputer. Maka dari itu para penjahat dunia maya kerap memanfaatkannya untuk menciptakan jaringan botnets yang besar.



- (2) Penyerang akan mengontrol atau meremote semua botnet untuk mengirimkan respon ke HTTP request ke aplikasi web (halaman website) yang dieksekusi server target.
- (3) Setelah itu server target berjalan dengan beban yang berat (overload) sampai tidak bisa lagi menampung koneksi dari user lain.

Dampak pada target aplikasi ketika DDoS ini dilakukan adalah:

- (1) Jumlah spam yang secara tiba-tiba meningkat. Yang mana pada waktu normal, jarang atau bahkan tidak ada spam yang mampir di website.

- (2) Website atau server yang menjadi lebih lambat. Dimana kamu membutuhkan waktu lebih lama dari biasanya dalam mengakses website maupun server.
- (3) Menyebabkan NULL Route (pemutusan rute network) pada IP Website atau server. Puncaknya, website atau server yang mengalami serangan ini tidak akan bisa diakses dalam jangka waktu tertentu.

## **Bagian 5. Brute Force**

Tujuan: Mahasiswa dapat menjelaskan apa yang terjadi jika hacker menggunakan sebuah aplikasi brute force dan target user menggunakan password default.

Tuliskan apa yang anda ketahui tentang Brute Force? Jelaskan bagaimana prosesnya teknik serangan ini untuk mendapatkan user dan password admin dari target Aplikasi? Serta jelaskan mengapa untuk security measure tidak boleh menggunakan password 1234 atau password yang terlalu singkat?

### **Jawab:**

Brute force adalah teknik peretasan agar bisa masuk ke dalam suatu sistem dengan cara menebak username dan password dengan mencoba-coba sampai menemukan kode yang tepat. Metode ini memang terlihat lebih sederhana tetapi peretas harus menggunakan strategi intelektual dengan merangkai kombinasi karakter yang berbeda sampai menemukan kombinasi yang benar.

Terdapat beberapa metode untuk serangan brute force:

- (1) Metode Sederhana. Penyerang akan menebak-nebak password yang mungkin dipakai pada akun target dengan mencoba kombinasi username password sebanyak mungkin. Terutama pada akun yang tidak menerapkan batasan login.
- (2) Metode Kamus. Penyerang telah menyiapkan sekumpulan password yang paling memungkinkan digunakan dan memulai mengeliminasi setiap daftar yang telah dicoba dan gagal. Artinya, hanya kombinasi password yang sering cocok saja yang digunakan sehingga lebih efisien dalam menjalankan aksinya.
- (3) Metode Hybrid. Penyerang telah memiliki daftar password untuk menebak login. Namun, selain mencoba menebak kombinasi pada daftar yang ada, mereka akan mencoba menambahkan angka atau huruf yang dianggap potensial.
- (4) Metode Credential. Penyerang menggunakan username dan password yang cocok pada suatu akun untuk akun lainnya karena tak sedikit orang yang menggunakan password yang sama dalam berbagai layanan. Sehingga dalam satu aksi pembobolan bisa banyak akun yang dikuasai.
- (5) Metode Rainbow Table. Penyerang tidak menebak password tapi melakukan dekripsi proteksi hash yaitu hasil enkripsi dari sebuah password yang lebih berpeluang memberikan password yang akurat

Dalam security measure tidak boleh menggunakan password 1234 atau password yang terlalu singkat dan diharapkan dapat lebih berhati-hati ketika membuat password pada akun atau sistem yang digunakan untuk menjaga keamanan dan mencegah peretasan brute force ini. Bahkan peretas dalam mendapatkan username dan password tidak hanya dapat menebak saja namun juga dapat menggunakan algoritma untuk mencoba dan menebak miliaran kata sandi hanya dalam waktu beberapa jam saja. Maka dari itu dalam membuat password perlu pertimbangan dan tidak asal, terutama password untuk akses sensitive yang menyimpan berbagai informasi dan aset penting.

## Bagian 6. SQL Injection

Tujuan: Mahasiswa dapat menjelaskan bagaimana vulnerability pada back end website dapat terjadi.

Tuliskan apa yang anda ketahui tentang SQL Injection? Jelaskan bagaimana prosesnya teknik serangan ini untuk mendapatkan informasi-informasi sensitive dari database web server? Dan aplikasi apa yang bisa digunakan untuk melakukan serangan ini?

### Jawab:

Sebagian besar situs web menggunakan database untuk menyimpan data. Aplikasi web membaca, memperbarui dan memasukkan data ke dalam database. Untuk melakukan interaksi dengan database dapat menggunakan SQL. SQL injection adalah sebuah teknik hacking untuk mendapatkan akses pada sistem database yang berbasis SQL.

SQL injection sangat berbahaya karena penyerang dapat mendapatkan akses ke database untuk mencuri data sensitive, memodifikasi data, membaca file lokal di luar www root atau login sebagai admin dan selanjutnya memanfaatkan sistem. Dalam SQL Injection penyerang akan memanfaatkan sisi kelemahan web seperti kurangnya penanganan terhadap karakter-karakter. Sehingga katakter tanda petik satu atau karakter double minus yang dapat menyebabkan suatu aplikasi dapat disisipi peretas dengan perintah SQL.

Cara kerja SQL injection cukup unik, penyerang dapat memanipulasi sistem dengan menambahkan karakter # sebagai commad, logika (OR, AND), karakter petik satu , karakter minus dan lainnya untuk memasuki database target. Contoh: `SELECT count (*) FROM Users WHERE Username='qwert' or 1=1 -- ' AND Password= 'zxcvb'`. Setelah itu sistem akan termanipulasi karena menganggap query tersebut sebagai syntax comment pada SQL, padahal sebenarnya query tersebut adalah kode serangan yang tereksekusi untuk memasuki akun tanpa mengetahui username dan passwordnya.

Berikut contoh aplikasi yang bisa digunakan untuk melakukan SQL Injection:

- SQLMAP
- HAVIJ
- SQLI DUMPER
- dan lainnya

## Bagian 7. XSS

Tujuan: Mahasiswa dapat menjelaskan bagaimana mekanisme cara kerja browser dan ketika browser tersebut diinject sebuah code.

Deskripsikan apa yang anda ketahui tentang XSS? Dan apa hubungannya XSS dengan browser injection? Serta apa yang terjadi ketika seseorang menyelipkan `<script>alert(1)</script>` ke dalam sebuah input form box? (Tuliskan minimal 1 paragraf)

### Jawab:

XSS (Cross-Site Scripting) adalah teknik serangan dimana penyerang menempatkan malicious client-end code ke laman web. Script dijalankan pada mesin client (user atau orang yang menggunakan web) bukan pada server maka dari itu ditulis dengan bahasa client seperti: JavaScript, VBScript, ActiveX, Flash, dan lainnya. Forum, kolom komentar, dan message boards biasanya digunakan oleh penyerang untuk memposting link untuk membuat skrip berbahaya. Skrip tersebut kemudian akan menyerang ketika korban mengklik tautan tersebut. Cross site scripting ini sering digunakan untuk mencuri session cookies, yang memungkinkan penyerang untuk menyamar sebagai korban. Dengan cara inilah, peretas bisa mengetahui data-data sensitif milik korban.

Hubungannya XSS dengan browser injection sangat erat karena mereka sama-sama menginjeksi dengan memasukan script berbahaya pada HTML dan JavaScript langsung ke situs web yang dikunjungi client.

Saya mencoba untuk menyelipkan `<script>alert(1)</script>` ke dalam sebuah input form box pada website DVWA dan mengeksekusinya yang terjadi adalah muncul popup angka 1 seperti pada gambar

