



Petunjuk Teknis

Konfigurasi Server dan Jaringan Laboratorium
Information Technology Security Assessment (ITSA)



DAFTAR ISI

DAFTAR ISI	1
DAFTAR TABEL	2
DAFTAR GAMBAR	3
INFORMASI DOKUMEN	4
LATAR BELAKANG	5
1. KONFIGURASI SERVER	6
1.1. SPESIFIKASI HARDWARE	6
1.2. INSTALASI MESIN VIRTUAL	7
1.3. INSTALASI SERVER TARGET	9
2. KONFIGURASI JARINGAN	15
2.1. SPESIFIKASI HARDWARE	15
2.2. SET UP WIFI AP	16
2.3. TOPOLOGI JARINGAN	18
3. PENUTUP	21
3.1. KESIMPULAN	21
3.2. SARAN	21
REFERENSI	22
LEMBAR PENGESAHAN	23

DAFTAR TABEL

Tabel 1. Spesifikasi <i>Hardware</i> Server Laboratorium ITSA D211.....	6
Tabel 2. Nama SSID dan Kata Sandi WiFi AP Laboratorium ITSA D211.....	17

DAFTAR GAMBAR

Gambar 1. Spesifikasi <i>Hardware</i> Server Laboratorium ITSA D211	6
Gambar 2. Tampilan Halaman <i>Website</i> Oracle VM VirtualBox	7
Gambar 3. Instalasi VirtualBox 6.1.26	8
Gambar 4. Informasi Tentang VirtualBox 6.1.26 yang Terinstal	8
Gambar 5. Tampilan Halaman Website Lokasi Unduh Metasploitable 2.....	9
Gambar 6. Tampilan Metasploitable 2.....	11
Gambar 7. Alamat IP Server Metasploitable 2	12
Gambar 8. Hasil Pemindaian Server Target Menggunakan Nmap	13
Gambar 9. Hasil Uji Coba Aplikasi Web Metasploitable 2	14
Gambar 10. AP TP-Link Archer C60 Laboratorium ITSA D211.....	15
Gambar 11. Spesifikasi Perangkat AP Laboratorium ITSA D211	16
Gambar 12. Set Up WiFi AP Laboratorium ITSA D211	17
Gambar 13. Topologi Jaringan Laboratorium ITSA D211	18
Gambar 14. Hasil Pemindaian pada Segmen Jaringan Laboratorium ITSA D211 ...	19

INFORMASI DOKUMEN

JUDUL	PETUNJUK TEKNIS KONFIGURASI SERVER DAN JARINGAN LABORATORIUM INFORMATION TECHNOLOGY SECURITY ASSESSMENT (ITSA)
VERSI	v1.0
TANGAL PENGESAHAN	11 Oktober 2021
TIM PENYUSUN	Kelompok Fungsi Operasi Identifikasi dan Proteksi Direktorat Operasi Keamanan Siber

LATAR BELAKANG

Banyaknya permintaan layanan ITSA yang masuk ke D211 dari Pemerintah Pusat maupun Pemerintah Daerah, maka personel D211 perlu mempersiapkan dirinya sehingga siap bertugas memberikan layanan ITSA yang berkualitas. Selain persiapan kondisi fisik tubuh yang sehat dan bugar, personel D211 juga perlu mempersiapkan kompetensi dan kapabilitasnya dalam melaksanakan ITSA. Salah satu kegiatan untuk mempersiapkan kompetensi personel adalah kegiatan latihan. Oleh sebab itu, dirasa perlu pembangunan sarana latihan untuk ITSA.

Laboratorium merupakan sarana yang dapat digunakan oleh personel D211 sebagai tempat untuk latihan dan mengasah keahlian. Selain itu, laboratorium juga dapat digunakan sebagai sarana untuk penelitian dan pengembangan kompetensi. Oleh sebab itu D211 membangun laboratorium khusus untuk latihan dan persiapan kegiatan ITSA sesuai dengan kebutuhan.

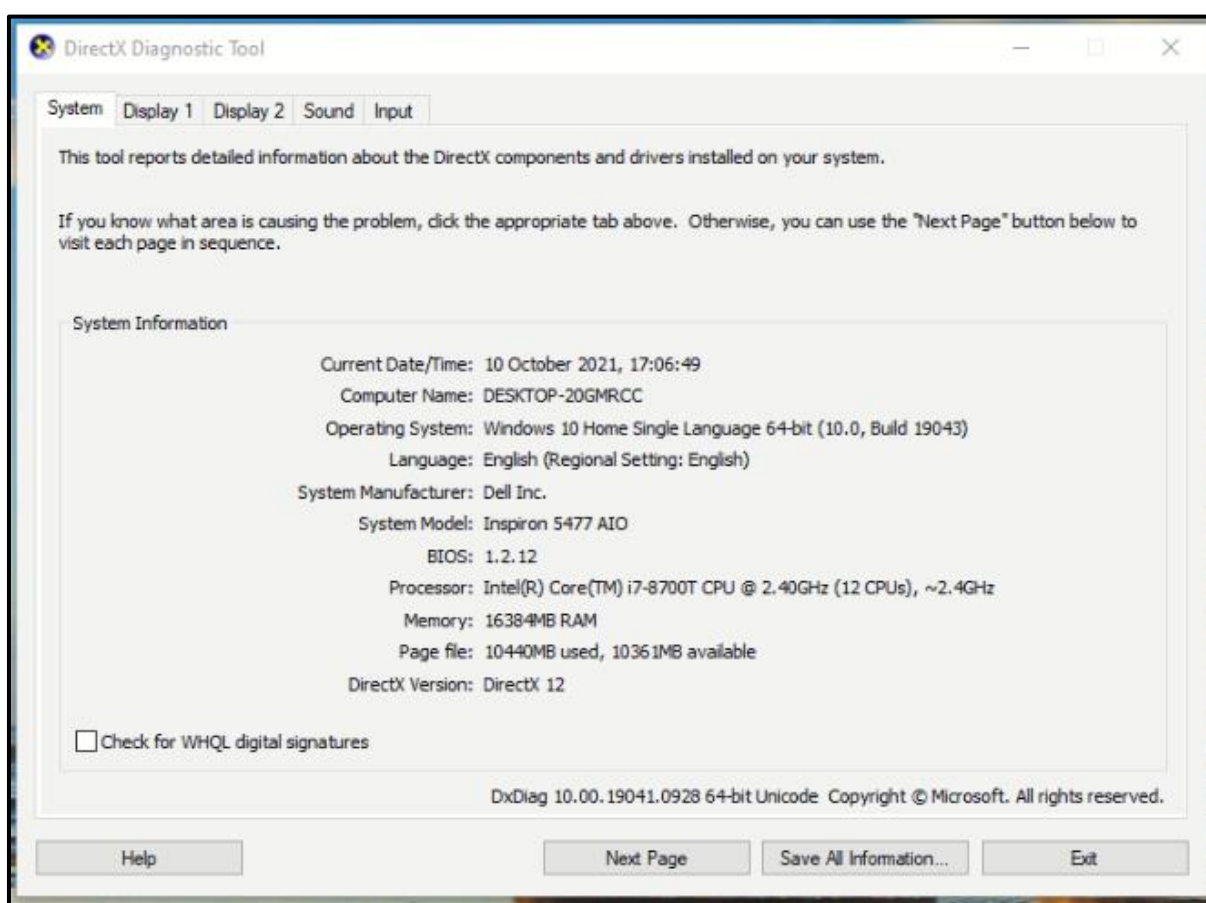
Laboratorium ITSA yang dibangun oleh D211 terdiri dari *hardware* dan *software*. Perangkat-perangkat yang digunakan dalam laboratorium disesuaikan dengan kebutuhan kompetensi untuk kegiatan ITSA. Laboratorium ITSA yang dibangun tersebut untuk latihan kegiatan ITSA Infrastruktur dan Aplikasi Web. Kegiatan ITSA Infrastruktur meliputi *security assessment* pada perangkat jaringan nirkabel (misalnya WiFi), perangkat jaringan (Router dan Switch), perangkat perimeter jaringan (Firewall, IPS, dan atau IDS), dan server layanan. Kegiatan ITSA Aplikasi Web meliputi *security assessment* pada aplikasi web itu sendiri. Oleh sebab itu, dalam pembangunan laboratorium ITSA tersebut dilakukan konfigurasi server dan jaringan untuk kegiatan latihan dan simulasi ITSA Infrastruktur dan Aplikasi Web.

Dalam dokumen juknis ini, *hardware* server dan jaringan yang digunakan adalah perangkat aset milik D211 yang ada saat ini. *Software* yang digunakan dalam laboratorium ITSA D211 bersumber dari *open source* yang dapat secara gratis diunduh di internet. Apabila di kemudian hari terdapat pembaruan *hardware* maupun versi *software* atau dilakukan pengembangan laboratorium sesuai kebutuhan, maka substansi dari dokumen juknis ini dapat berubah sesuai dengan kondisi laboratorium ITSA D211 terbaru.

1. KONFIGURASI SERVER

1.1. SPESIFIKASI HARDWARE

Hardware server yang digunakan adalah komputer personal (PC) milik D211. PC yang digunakan sebagai server bermerek Dell dengan sistem operasi yang terinstal adalah Windows 10. PC tersebut didukung oleh prosesor Intel Core i7. Pada Gambar 1 dan Tabel 1 disajikan informasi rinci spesifikasi PC yang digunakan sebagai server laboratorium ITSA D211.



Gambar 1. Spesifikasi *Hardware* Server Laboratorium ITSA D211

Tabel 1. Spesifikasi *Hardware* Server Laboratorium ITSA D211

Merek Perangkat	Dell Inspiron 5477 AIO
Sistem Operasi	Windows 10 Home Single Language 64-bit
Prosesor	Intel(R) Core(TM) i7-8700T CPU @ 2.40GHz (12 CPUs)
RAM	16384 MB

1.2. INSTALASI MESIN VIRTUAL

Server layanan (termasuk aplikasi web) yang digunakan sebagai target ITSA pada laboratorium dikonfigurasi di dalam mesin virtual. Hal tersebut bertujuan untuk efisiensi sumber daya perangkat PC yang digunakan. Oleh sebab itu, dalam bagian ini disajikan instalasi mesin virtual.

Dalam pembangunan laboratorium ITSA D211 menggunakan Oracle VM VirtualBox sebagai *hypervisor* yang menjalankan mesin virtual server target. Oracle VM VirtualBox adalah aplikasi virtualisasi lintas *platform*. VirtualBox adalah produk virtualisasi x86 dan AMD64/Intel64 yang kuat untuk perusahaan maupun penggunaan di rumah [1]. VirtualBox tidak hanya merupakan produk yang sangat kaya fitur dan berkinerja tinggi untuk pelanggan perusahaan, tetapi juga satu-satunya solusi profesional yang tersedia secara bebas sebagai Perangkat Lunak Sumber Terbuka di bawah persyaratan GNU General Public License (GPL) versi 2. *Installer* aplikasi VirtualBox dapat diunduh di *website* resminya. Pada Gambar 2 disajikan tampilan halaman *website* Oracle VM VirtualBox.

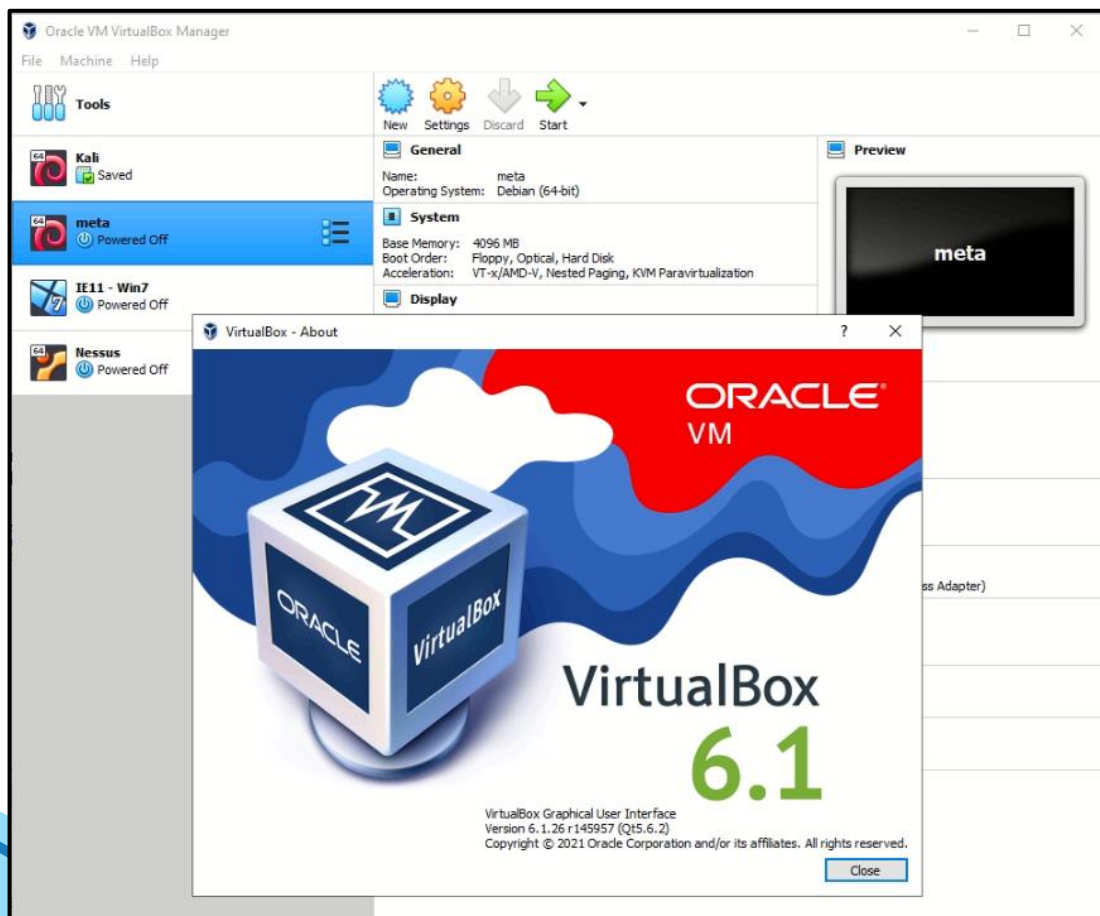


Gambar 2. Tampilan Halaman *Website* Oracle VM VirtualBox

Dalam laboratorium ITSA D211 menggunakan VirtualBox 6.1.26. Setelah *file installer* VirtualBox berhasil diunduh, maka selanjutnya dilakukan proses instalasi. Pada Gambar 3 disajikan instalasi VirtualBox 6.1.26. Setelah proses instalasi selesai, maka VirtualBox siap digunakan untuk menjalankan mesin virtual server target. Pada Gambar 4 disajikan informasi tentang VirtualBox 6.1.26 yang terinstal.



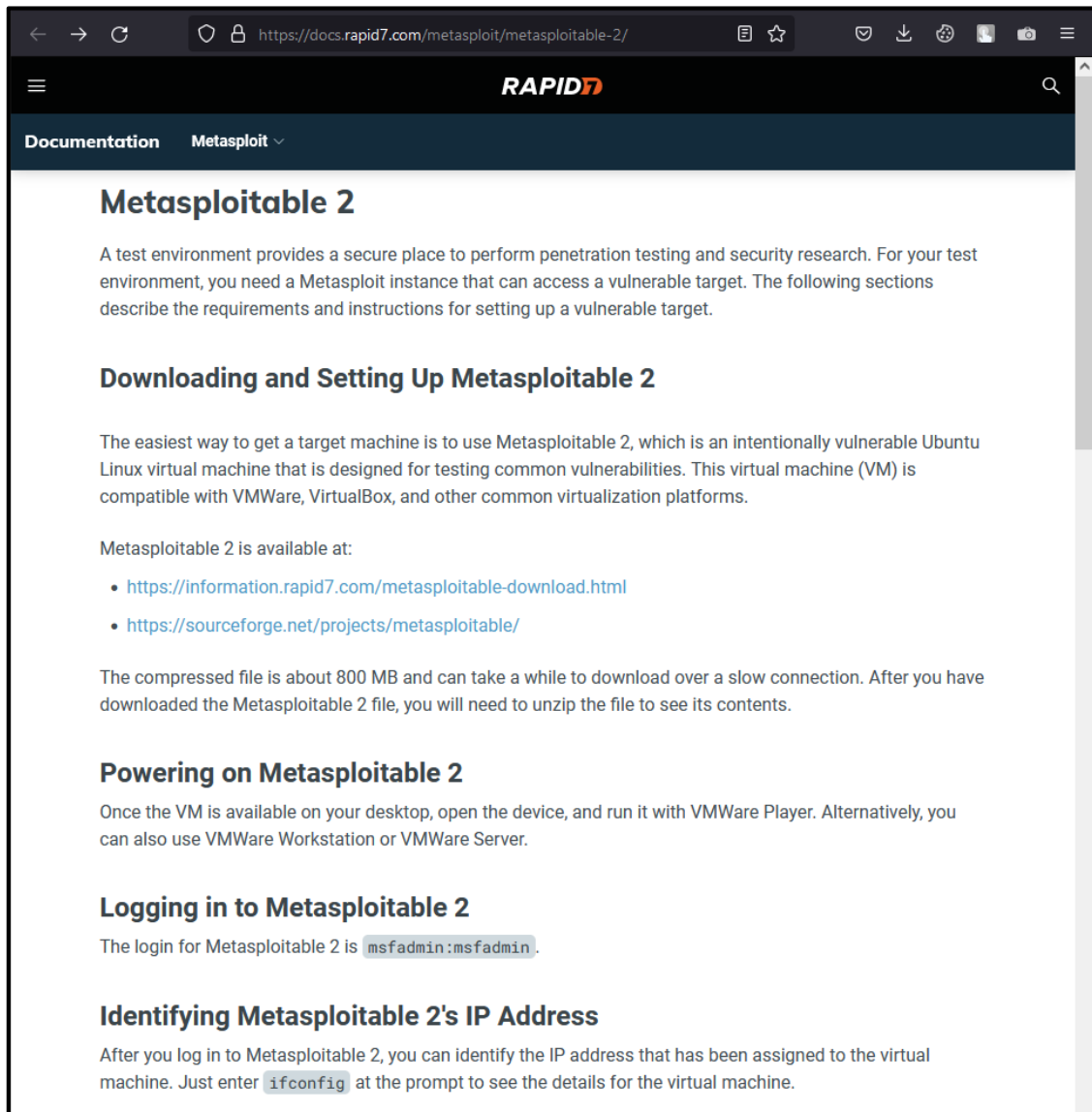
Gambar 3. Instalasi VirtualBox 6.1.26



Gambar 4. Informasi Tentang VirtualBox 6.1.26 yang Terinstal

1.3. INSTALASI SERVER TARGET

Server target yang digunakan untuk latihan dalam laboratorium ITSA D211 adalah Metasploitable 2. Mesin virtual server Metasploitable 2 dapat diunduh pada *website* Rapid7 [2]. Pada Gambar 5 disajikan tampilan halaman Rapid7 tempat untuk mengunduh mesin virtual server Metasploitable 2.

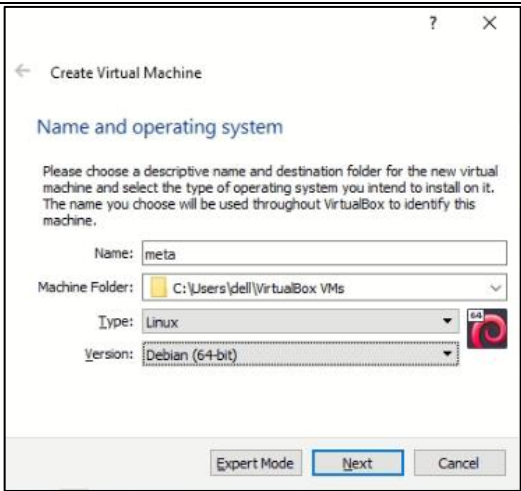
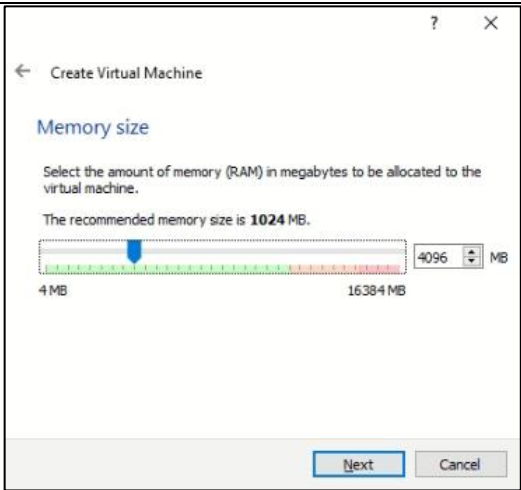
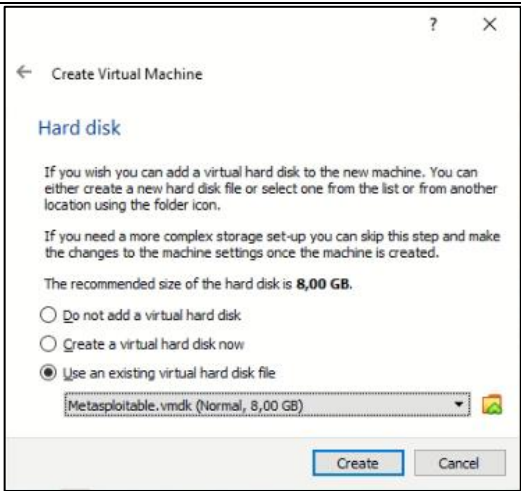


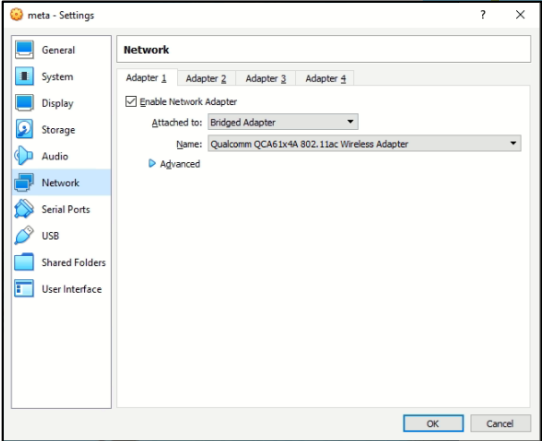
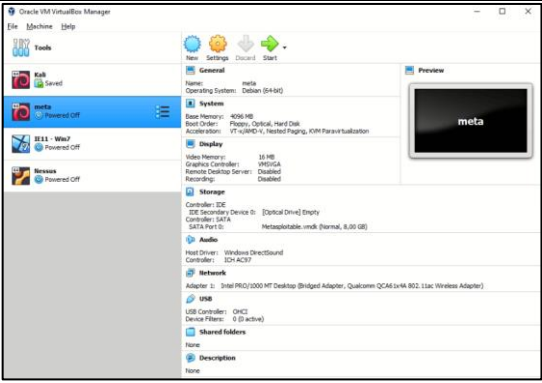
Gambar 5. Tampilan Halaman Website Lokasi Unduh Metasploitable 2

Setelah *file* mesin virtual server Metasploitable 2 berhasil diunduh, maka selanjutnya dilakukan proses pembuatan mesin virtual pada VirtualBox. *File* mesin virtual server Metasploitable 2 berupa Virtual Machine Disk Format (.vmdk) yang mana langsung dapat diimpor ke VirtualBox dan langsung dapat dijalankan. Pada

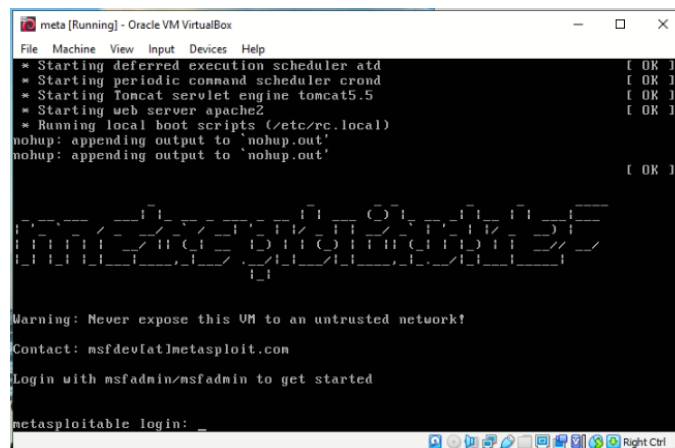
Tabel 2 disajikan proses konfigurasi mesin virtual server Metasploitable 2 pada VirtualBox laboratorium ITSA D211.

Tabel 2. Proses Konfigurasi Mesin Virtual Server Metasploitable 2

Proses ke	Aktivitas	Gambar
1	Membuat mesin virtual baru, memberi nama dan memilih tipe serta versi mesin.	
2	Mengalokasikan RAM.	
3	Memilih Hard disk Metasploitable.vmdk kemudian Create.	

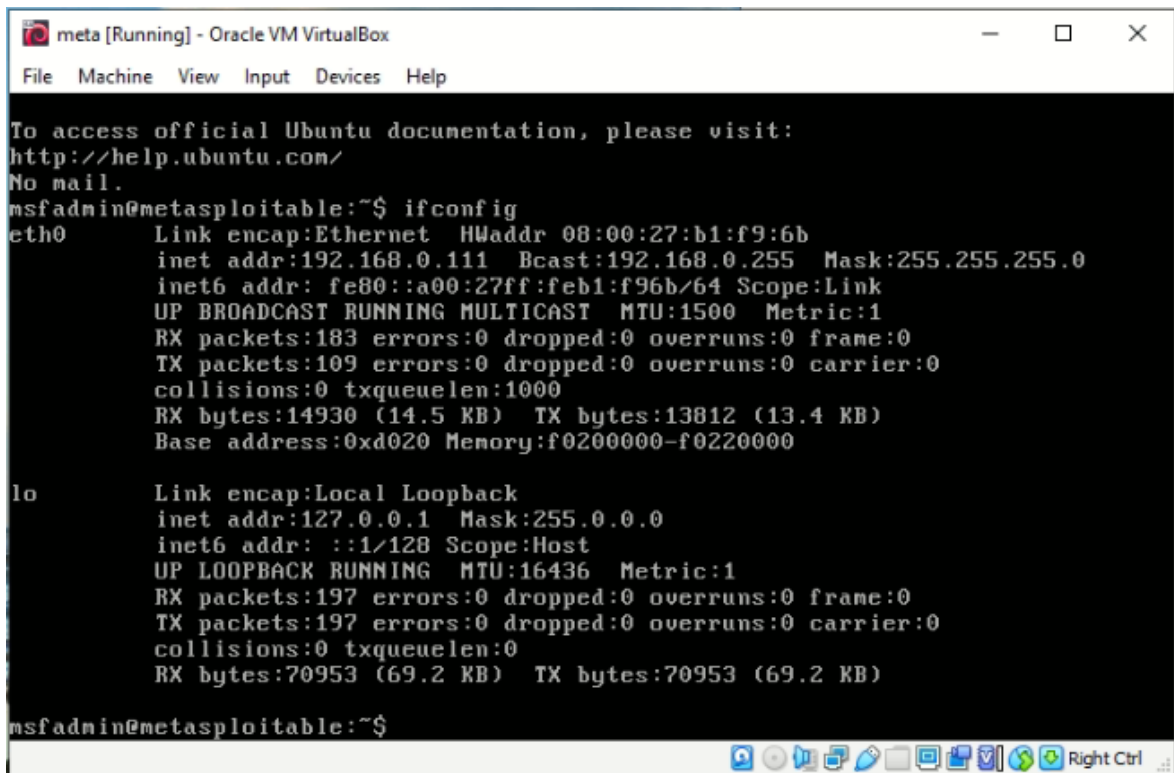
4	Mengatur antar muka jaringan mesin virtual server Metasploitable 2 menjadi mode Bridge Adapter sehingga mendapatkan alamat IP yang satu segmen dalam jaringan AP laboratorium ITSA D211.	
5	Server Metasploitable 2 siap untuk dijalankan.	

Setelah proses instalasi server Metasploitable 2 selesai, maka selanjutnya server tersebut siap untuk dijalankan sebagai target serangan dalam latihan ITSA Infrastruktur dan Aplikasi Web. Metasploitable 2 merupakan server berbasis sistem operasi Linux yang sengaja dibuat dengan banyak kerentanan yang dapat dieksploitasi. Metasploitable 2 diperuntukkan sebagai server target untuk latihan uji penetrasi (pentest). Pada Gambar 6 disajikan tampilan Metasploitable 2.



Gambar 6. Tampilan Metasploitable 2

Setelah Metasploitable 2 berhasil dijalankan, maka selanjutnya masuk ke server Metasploitable 2 dengan *username* “**msfadmin**” dan *password* “**msfadmin**”. Setelah berhasil masuk ke server Metasploitable 2, maka selanjutnya menjalankan perintah “**ifconfig**” untuk memeriksa alamat IP Metasploitable 2. Pada Gambar 7 disajikan informasi alamat IP server Metasploitable 2.



```
meta [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b1:f9:6b
          inet addr:192.168.0.111  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb1:f96b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14930 (14.5 KB)  TX bytes:13812 (13.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:197 errors:0 dropped:0 overruns:0 frame:0
          TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:70953 (69.2 KB)  TX bytes:70953 (69.2 KB)

msfadmin@metasploitable:~$
```

Gambar 7. Alamat IP Server Metasploitable 2

Pada Gambar 7 menampilkan alamat IP server Metasploitable 2 yaitu 192.168.0.111. Selanjutnya setelah itu dilakukan uji pemindaian (*scanning*) server target oleh perangkat penguji untuk memastikan bahwa perangkat penguji dapat berkomunikasi dengan server target dan melakukan uji coba penetrasi. Penguji melakukan uji koneksi menggunakan perangkat yang terinstal sistem operasi Kali Linux dan melakukan pemindaian menggunakan aplikasi Nmap. Pada Gambar 8 disajikan hasil pemindaian server target menggunakan Nmap oleh penguji.



```
Nmap scan report for 192.168.0.111
Host is up (0.058s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
```

Gambar 8. Hasil Pemindaian Server Target Menggunakan Nmap

Pada Gambar 8 menampilkan hasil pemindaian server target dan menunjukkan bahwa server memiliki banyak port layanan yang terbuka (*open*). Hasil pemindaian tersebut dapat digunakan oleh penguji sebagai bahan informasi untuk melakukan eksplorasi lanjutan dan menentukan exploit yang akan digunakan untuk melakukan uji penetrasi. Selain itu, dari hasil pemindaian tersebut juga diperoleh informasi bahwa port 80 di server target terbuka. Hal itu menandakan bahwa layanan aplikasi web di server target dapat diakses melalui web browser. Oleh sebab itu, selanjutnya dilakukan uji coba akses aplikasi web yang ada pada server target menggunakan web browser. Pada Gambar 9 disajikan hasil uji coba akses aplikasi web tersebut menggunakan web browser.



Gambar 9. Hasil Uji Coba Aplikasi Web Metasploitable 2

Gambar 9 menunjukkan hasil uji coba akses aplikasi web pada server Metasploitable 2 dan menampilkan bahwa di aplikasi web tersebut terdapat aplikasi Damn Vulnerable Web App (DVWA). Aplikasi DVWA tersebut dapat digunakan oleh para personel D211 untuk latihan ITSA Aplikasi Web. Setelah server target (Metasploitable 2) berhasil dikonfigurasi dan dilakukan uji coba akses, maka server tersebut siap untuk digunakan sebagai target latihan uji penetrasi oleh para personel D211 guna persiapan ITSA Infrastruktur dan Aplikasi Web.

2. KONFIGURASI JARINGAN

2.1. SPESIFIKASI HARDWARE

Perangkat jaringan yang digunakan dalam laboratorium ITSA D211 adalah Wireless Router Acces Point (AP) TP-Link Archer C60. Semua perangkat yang terkait (termasuk perangkat penguji, klien, dan server) dalam laboratorium terhubung dan dapat saling berkomunikasi melalui AP tersebut. Pada Gambar 10 disajikan tampilan AP yang digunakan.



Gambar 10. AP TP-Link Archer C60 Laboratorium ITSA D211

AP TP-Link Archer C60 merupakan Wireless Dual Band Router (2.4GHz dan 5GHz). AP tersebut merupakan salah satu perangkat jaringan yang dimiliki D211. Pada Gambar 11 disajikan spesifikasi perangkat AP Laboratorium ITSA D211.

DRAFT PETUNJUK TEKNIS KONFIGURASI SERVER DAN JARINGAN LABORATORIUM ITSA



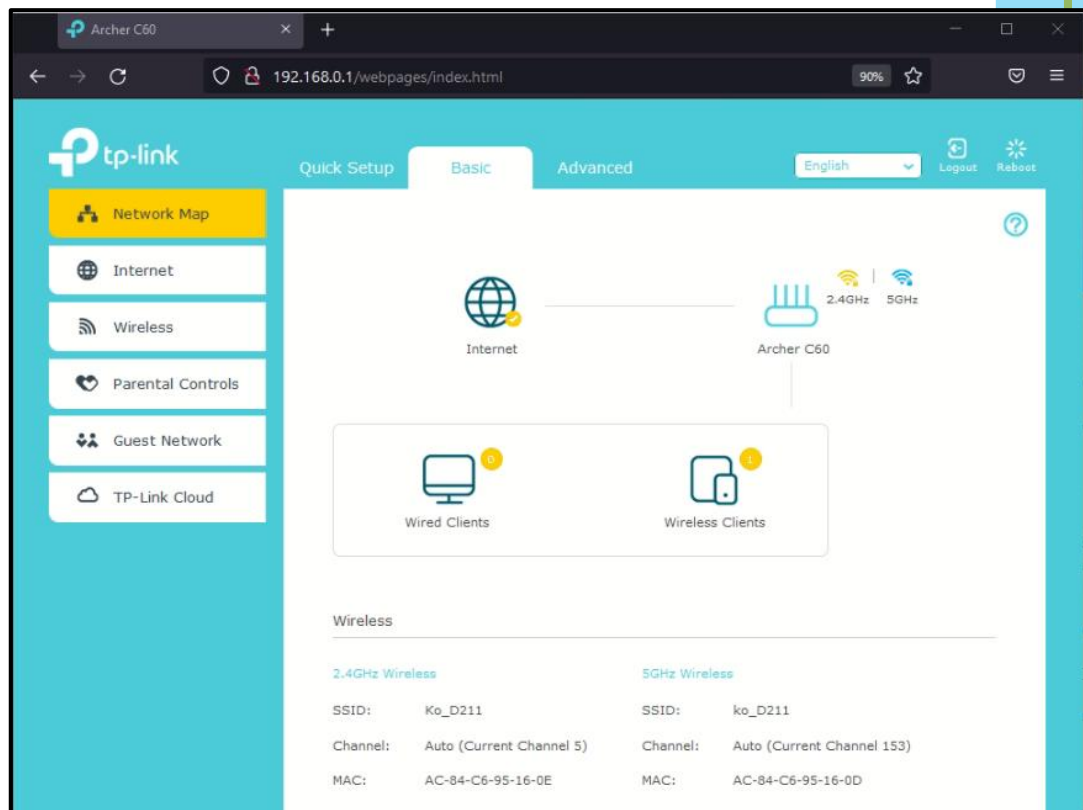
Gambar 11. Spesifikasi Perangkat AP Laboratorium ITSA D211

2.2. SET UP WIFI AP

Supaya dapat digunakan, AP Laboratorium ITSA D211 perlu dipersiapkan (set up). AP TP-Link Archer C60 memungkinkan untuk jaringan kabel dan nirkabel (WiFi). Pada Gambar 12 disajikan set up WiFi AP Laboratorium ITSA D211. Pada Tabel 2 disajikan nama Service Set Identifier (SSID) beserta kata sandinya.

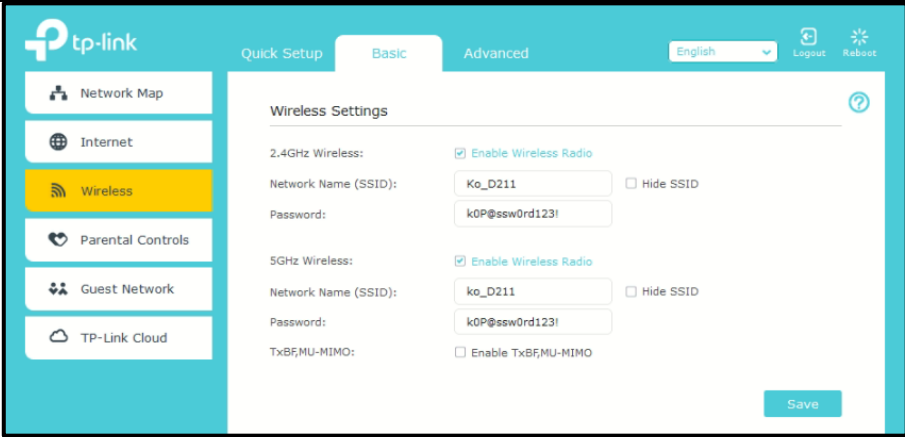
DRAFT PETUNJUK TEKNIS KONFIGURASI SERVER DAN JARINGAN LABORATORIUM ITSa

...



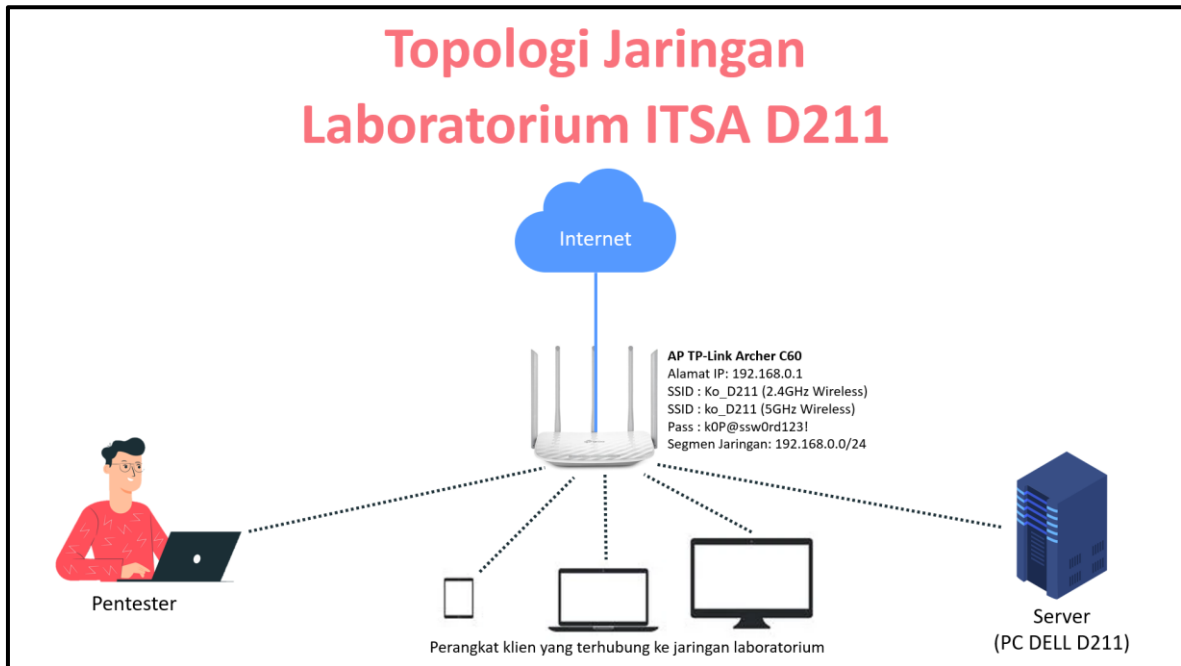
Gambar 12. Set Up WiFi AP Laboratorium ITSA D211

Tabel 2. Nama SSID dan Kata Sandi WiFi AP Laboratorium ITSA D211

	
2.4GHz Wireless:	
SSID	Ko_D211
Kata sandi	k0P@ssw0rd123!
5GHz Wireless:	
SSID	ko_D211
Kata sandi	k0P@ssw0rd123!

2.3. TOPOLOGI JARINGAN

Topologi jaringan adalah gambaran struktur fisik dan logika suatu jaringan. Topologi jaringan digunakan untuk memudahkan dalam mendesain koneksi suatu jaringan. Pada Gambar 13 disajikan topologi jaringan laboratorium ITSA D211.



Gambar 13. Topologi Jaringan Laboratorium ITSA D211

Setiap perangkat yang terhubung ke jaringan AP laboratorium ITSA D211 akan secara otomatis mendapatkan alamat IP secara dinamik (DHCP). Antarmuka jaringan mesin virtual server target dikonfigurasi mode Bridge Adapter sehingga mendapatkan alamat IP yang satu segmen dalam jaringan AP laboratorium ITSA D211. Pada saat perangkat pengujian terhubung ke AP, maka akan secara otomatis akan mendapatkan alamat IP dan bisa berkomunikasi dengan klien lain (termasuk server target) yang terhubung dalam jaringan tersebut.

Selanjutnya, untuk memastikan bahwa jaringan laboratorium ITSA D211 yang telah dibangun berfungsi dengan baik, maka dilakukan uji coba pemindaian untuk memastikan bahwa pengujian dapat melakukan pemindaian terhadap semua perangkat yang terhubung dalam satu jaringan tersebut dan selanjutnya dapat berkomunikasi dan melakukan uji coba penetrasi. Uji coba pemindaian perangkat yang terkoneksi dalam satu segmen jaringan laboratorium ITSA D211

menggunakan Nmap dalam perangkat penguji. Pada Gambar 14 disajikan hasil pemindaian satu segmen jaringan laboratorium ITSA D211.

```
(kali㉿kali)-[~]
$ nmap 192.168.0.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 05:00 EDT
Nmap scan report for 192.168.0.1
Host is up (0.015s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1900/tcp   open  upnp

Nmap scan report for 192.168.0.111
Host is up (0.058s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap scan report for 192.168.0.186
Host is up (0.000075s latency).
All 1000 scanned ports on 192.168.0.186 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 41.27 seconds

(kali㉿kali)-[~]
$
```

Gambar 14. Hasil Pemindaian pada Segmen Jaringan Laboratorium ITSA D211

Pada Gambar 14 menampilkan hasil pemindaian perangkat yang terkoneksi dalam satu segmen jaringan laboratorium ITSA D211 dan hasilnya menunjukkan bahwa terdapat 2 (dua) perangkat yang memiliki alamat IP dalam satu segmen jaringan tersebut beserta port layanannya yang terbuka. Perangkat yang terdeteksi dengan alamat IP 192.168.0.1 adalah perangkat WiFi AP yang merupakan *gateway* koneksi jaringan laboratorium ITSA D211 ke internet, dan perangkat yang terdeteksi dengan alamat IP 192.168.0.111 adalah perangkat mesin virtual server

target (Metasploitable 2). Dari hasil pemindaian tersebut, maka dapat disimpulkan bahwa jaringan laboratorium ITSA D211 bekerja dengan baik dan seluruh perangkat yang terkoneksi di dalamnya (termasuk server Metasploitable 2) dapat diakses oleh perangkat penguji.

3. PENUTUP

3.1. KESIMPULAN

Telah dilakukan pembangunan laboratorium ITSA di D211 beserta pembuatan dokumen juknis konfigurasi server dan jaringannya. Laboratorium ITSA dibangun guna memenuhi kebutuhan sarana latihan personel D211 dalam mempersiapkan kompetensi dan kapabilitasnya untuk melaksanakan tugas ITSA. Laboratorium ITSA yang dibangun tersebut untuk latihan kegiatan ITSA Infrastruktur dan Aplikasi Web. Laboratorium ITSA yang dibangun oleh D211 terdiri dari *hardware* dan *software*. *Hardware* yang digunakan dalam laboratorium merupakan aset milik D211 dan *software* yang digunakan dalam pembangunan laboratorium tersebut bersumber dari *open source*. *Hardware* yang digunakan sebagai perangkat server adalah PC bermerek Dell Inspiron 5477 AIO dan perangkat yang digunakan sebagai router jaringan Laboratorium ITSA D211 adalah Wireless Router AP TP-Link Archer C60. *Software* yang digunakan untuk server target adalah Oracle VM VirtualBox dan mesin virtual server target yang digunakan adalah Metasploitable 2. Setelah dilakukan konfigurasi server dan jaringan, kemudian dilakukan uji coba koneksi dengan hasil server dan jaringan dapat terhubung dan bekerja dengan baik, maka Laboratorium ITSA D211 siap digunakan oleh para personel untuk latihan ITSA Infrastruktur dan Aplikasi Web.

3.2. SARAN

Laboratorium ITSA yang dibangun oleh D211 saat ini peruntukannya untuk latihan ITSA Infrastruktur dan Aplikasi Web dengan spesifikasi *hardware* terbatas yang dimiliki oleh D211. Untuk memenuhi kebutuhan kompetensi personel dan permintaan ITSA yang bervariasi (tidak hanya terbatas pada ITSA Infrastruktur dan Aplikasi Web) serta seiring berkembangnya teknologi yang digunakan oleh *stakeholders* BSSN (Pemerintah Pusat dan Daerah), maka perlu dilakukan pengembangan laboratorium ITSA D211. Pengembangan laboratorium dapat berupa peningkatan kuantitas dan kualitas spesifikasi *hardware* yang digunakan. Selain itu juga perlu dilakukan pengembangan *software* yang digunakan berupa penambahan server dan aplikasi *mobile* maupun *desktop* sehingga laboratorium ITSA D211 dapat mengakomodasi untuk kegiatan latihan dan persiapan ITSA Aplikasi Mobile dan Desktop.


REFERENSI

- [1] "Welcome to VirtualBox.org!," *Oracle VM VirtualBox*. [Online]. Available: <https://www.virtualbox.org/>. [Accessed: 11-Oct-2021].
- [2] "Metasploitable 2," *Metasploitable 2 | Metasploit Documentation*. [Online]. Available: <https://docs.rapid7.com/metasploit/metasploitable-2/>. [Accessed: 11-Oct-2021].

LEMBAR PENGESAHAN

PETUNJUK TEKNIS
KONFIGURASI SERVER DAN JARINGAN LABORATORIUM ITSa

Telah disahkan oleh:

<p>Direktur Operasi Keamanan Siber</p> <div><p>Ditandatangani Secara Elektronik oleh : DIREKTUR OPERASI KEAMANAN SIBER</p><p>Ferdinand Mahulette, S.E. Brigadir Jenderal TNI</p></div> <p>Ferdinand Mahulette, S.E</p>	<p>Koordinator Kelompok</p> <p>Satryo Suryantoro, S.Sos</p>
--	---

KELOMPOK FUNGSI OPERASI IDENTIFIKASI DANN PROTEKSI
DIREKTORAT OPERASI KEAMANAN SIBER
BADAN SIBER DAN SANDI NEGARA